

Public Redacted Version of the Rebuttal Report of Georgios Zervas, Ph.D

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

IN RE META PIXEL TAX FILING CASES

This document relates to:
Case No. 5:22-cv-07557-PCP, All actions

Case No. 5:22-cv-07557-PCP

**DEFENDANT META PLATFORMS,
INC.’S OPPOSITION TO
PLAINTIFFS’ MOTION FOR CLASS
CERTIFICATION**

Date: January 15, 2026
Time: 10:00 a.m.
Courtroom 8, 4th Floor

Date Action Filed: Dec. 1, 2022
Hon. P. Casey Pitts

CORRECTED REBUTTAL EXPERT REPORT OF GEORGIOS ZERVAS, PH.D.

OCTOBER 27, 2025

TABLE OF CONTENTS

I.	Introduction.....	1
A.	Qualifications.....	1
B.	Assignment	3
C.	Facts and Data Considered.....	5
D.	Summary of Plaintiffs’ Allegations	5
II.	Summary of Opinions.....	7
III.	Background.....	9
A.	The Meta Pixel.....	11
	1. What the Meta Pixel Is and How It Operates	11
	2. Event Data Generated by Developers’ Use of the Meta Pixel.....	15
B.	Cookies	19
C.	Tag Managers and Consent Management Platforms	21
D.	Conversions API.....	23
E.	Meta’s Technical Measures	26
	1. Detection and Filtration	27
	2. Core Setup.....	32
	3. Notifications.....	37
IV.	Plaintiffs’ Experts’ Proposed Methodologies for Counting Visits to the H&R Block and TaxAct Websites Are Flawed.....	38
A.	The Proposed Methodologies for Counting Visits to the H&R Block and TaxAct Websites Are Unreliable	40
	1. Mr. Zeidman’s Assumption that Each [REDACTED] Equates to a Unique Website Visit is Unsupported.....	40
	2. Methodologies for Counting Visits to the H&R Block and TaxAct Websites Count Visits from Non-Humans	42
B.	The Proposed Methodologies for Counting Visits to the H&R Block and TaxAct Websites Cannot Be Used to Exclude Visits from Users Who Provided Consent	42
C.	Methodologies for Counting Visits to the H&R Block and TaxAct Websites Cannot Be Used to Count Visits from Individuals in California	43
V.	Plaintiffs’ Experts’ Proposed Methodologies to Count Website Visits Are Incapable of Accurately Identifying Visitors to the H&R Block and TaxAct Websites.....	48

VI.	Mr. Zeidman’s Opinion that He Found an “Enormous Amount of Tax Information” and Other Data Transmitted to Meta is Unreliable.....	52
A.	Mr. Zeidman’s Opinions Contain Significant Methodological Flaws.....	53
B.	My Independent Review Shows that the Event Data Mr. Zeidman Analyzed Appears Infrequently	55
VII.	Mr. Zeidman Failed to Consider Variability in The Data Developers Transmit Via the Meta Pixel.....	57
A.	Users Have Controls That Prevent or Limit the Transmission of Data via the Meta Pixel	58
	1. Users Can Employ Ad Blockers or Other Browser Extensions that Prevent Data Transmissions	58
	2. Users Can Grant or Deny Website-Specific Consent for Certain Tracking Technologies.....	62
	3. Users Could Have Previously Visited a Meta Domain or Can Be Logged In to a Meta User Account, Affecting Cookie Transmission	67
	4. Users Can Adjust Browser-Specific Controls or Use Browsers that Affect What Data Can Be Sent Via the Meta Pixel	69
	5. Users Can Visit Websites with Strict or Private Browsing Modes that Block the Transmission of Data via the Meta Pixel	73
B.	Developers Have Controls That Limit or Modify the Data They Can Transmit Via the Meta Pixel, and the TaxAct and H&R Block Websites Used Those Controls in Ways that Affected Their Transmission of Data	78
	1. Developers Choose Whether to Send Events and Parameters to Meta	80
	2. Developers Can Disable Transmission of Automatic Events	82
	3. Developers Selected What Webpages Should Generate Events.....	85
	4. Developers Selected the Browsers for Whom to Generate and Send Event Data to Meta.....	86
C.	Meta’s Detection and Filtration Code Varied Over Time	87
VIII.	Mr. Zeidman Ignored Controls that Meta Provides to Its Users to Limit Meta’s Use of Data Sent As a Result of Developers’ Use of the Meta Pixel for Advertising Purposes	88
IX.	Mr. Zeidman Mischaracterized the Technical Nature of the Alleged Pen Register Data.....	94

I. INTRODUCTION

A. Qualifications

1. I am an Associate Professor of Marketing at Boston University Questrom School of Business, a founding member of the Faculty of Computing & Data Sciences, a Director of Online Initiatives and Innovation for BU Virtual and the Faculty of Computing and Data Sciences (“CDS”), and Affiliated Faculty of the Department of Computer Science. I was also a visiting researcher at Microsoft Research New England. Prior to joining the Boston University faculty, I held various academic roles, including visiting scholar at the MIT Sloan School of Management, Simons Postdoctoral Fellow at Yale University, and affiliate at the Center for Research on Computation and Society at Harvard University’s John A. Paulson School of Engineering and Applied Sciences. I am an associate editor of ACM Transactions on Economics and Computation, and I sit on the editorial review boards of Marketing Science and the Journal of Marketing. At Boston University, I teach the course Machine Learning for Business Analytics at the undergraduate and graduate levels.

2. My research combines methods from computer science and economics to study online marketplaces to understand their impact on consumer and firm behavior. I have conducted studies of online marketplaces such as Airbnb, Yelp, TripAdvisor, and Expedia. My work is empirical in nature and includes assembling and analyzing novel sources of data that I collect from these marketplaces to study their operation. I hold a Bachelor of Engineering and a Master of Science in Computer Science from Imperial College London, a Master of Arts in Interactive Media from London College of Communication, and a Ph.D. in Computer Science from Boston University. Before pursuing my Ph.D. in Computer Science, I ran a small information technology

company. My C.V. is attached as **Appendix A**, and a list of my prior testimony in the last four years is attached as **Appendix B**.

3. I have experience with internet technologies, similar to those involved in this matter, including through professional and academic experience, and my work as an expert witness in other litigations, including testifying in a Federal Court trial.¹ I have analyzed web browsing session data as part of my research.² I also have professional and academic experience, both writing and reviewing source code, including in the programming languages used in this case. In my prior work³ as an expert witness, I have also explained modern third-party tools, like the Meta Pixel, Google Analytics, and Google Ads, that website developers may rely on, including what data may be transmitted as a result of the operation of these tools and how such data may be used for analytics and advertising services.⁴

4. I also have experience with the specific technologies at issue in this case through my work as an expert witness in another litigation. I submitted a report in the matter of *Angel McDaniel, et al. v. Meta Platforms, Inc.*, in the Superior Court of the State of California for the County of Santa Clara, Case No. 21-cv-383231. In that matter, I explained the Meta Pixel, including its purpose, how it functions, and why it is widely used across the Internet. I also analyzed Meta Pixel code that Meta made available for inspection, as well as sample data produced in the litigation,

¹ See **Appendix B** (“*Frasco et al. v. Flo Health, Inc., Google LLC, Meta Platforms, Inc., AppsFlyer, Inc., and Flurry, Inc.*, Case No. 3:21-cv-00757-JD (“*Frasco et al. v. Flo Health et al.*”)”).

² See, e.g., Armona, Luis, et al., “Learning Product Characteristics and Consumer Preferences from Search Data,” *Marketing Science*, 44(4), 2024, pp. 838–855, p. 841, (“We make use of a session ID variable recorded by IE that captures the URLs visited by a single user during one continuous “session” defined as continuous usage of their computer where the time between clicks is no more than 30 minutes.”); Budak, Ceren, et al., “Understanding Emerging Threats to Online Advertising,” *EC’16: Proceedings of the 2016 ACM Conference on Economics and Computation*, July 21, 2016, pp. 561–578, p. 565 (“When a user visits any one of these top 10,000 retailers, we call that visit, along with all subsequent, uninterrupted visits on the same domain, a single shopping session.”).

³ See **Appendix B**.

⁴ See, e.g., **Appendix B** (“*Frasco et al. v. Flo Health et al.; Brown et al. v. Google, LLC*, Case No. 4:20-cv-03664-YGR; *Calhoun et al. v. Google LLC, U.S.*, Case No. 5:20-cv-05146-YGR-SVK.”).

including event data transmitted via the Meta Pixel and Conversions API and subsequently stored within Meta’s databases.

5. I am being compensated at the rate of \$950 per hour for my time working on this case. Research and analysis for this report was also performed by Analysis Group, Inc. personnel under my direction and guidance. In addition, I receive a portion of the fees paid to Analysis Group, Inc. for its work. This compensation is not contingent on the nature of my findings or the outcome of this litigation.

B. Assignment

6. I was retained by Gibson, Dunn & Crutcher, LLP and Latham & Watkins LLP (“Counsel”) on behalf of Meta Platforms, Inc., formerly known as Facebook, Inc. (“Meta,” “Facebook,” or “Defendant”) to provide expert testimony about the relevant technologies, including those related to the generation and transmission of data, in the matter of *In re Meta Pixel Tax Filing Cases*, pending in the United States District Court for the Northern District of California San Jose Division, Case No. 5:22-cv-07557-PCP.

7. On August 18, 2025, plaintiffs’ experts Robert Zeidman and Colin Weir submitted expert reports on behalf of plaintiffs (“Zeidman Report” and “Weir Report,” respectively).⁵ Counsel asked me to review the Zeidman Report and the Weir Report and evaluate their analyses and opinions on topics that fall within my areas of expertise. More specifically, I was asked to:

- a. Explain how relevant technologies related to modern web communications, including technologies like pixels (which are snippets of code) for analytics and advertising, operate.
- b. Explain how the Meta Pixel and Conversions API operate.

⁵ Expert Report of Robert Zeidman, *In re Meta Pixel Tax Filing Cases*, Case No. 5:22-cv-07557-PCP, August 18, 2025 (“Zeidman Report”); Expert Report of Colin B. Weir, *In re Meta Pixel Tax Filing Cases*, Case No. 5:22-cv-07557-PCP, August 18, 2025 (“Weir Report”).

- c. Explain Meta’s efforts to detect and filter potentially “sensitive”⁶ data transmitted to Meta’s servers from developers who use the Meta Pixel and/or Conversions API.
- d. Assess the reliability of Mr. Zeidman’s and Mr. Weir’s proposed methodologies to count the number of visits to the H&R Block and TaxAct websites during the proposed class periods and whether those proposed methodologies can be used to: (1) exclude visits to the H&R Block and TaxAct websites from website visitors who consented to cookies during the proposed class periods; (2) identify the locations of website visitors when they accessed the H&R Block or TaxAct websites during the proposed class periods; and (3) identify visitors to the H&R Block and TaxAct websites during the proposed class periods.
- e. Evaluate Mr. Zeidman’s opinions that: (1) “the Meta Pixel operated in a largely uniform manner” on the H&R Block and TaxAct websites “with respect to the basic mechanics of collecting and transmitting visitor data to Meta;”⁷ and (2) he “found an enormous amount of tax information and other data transmitted to Meta from the Tax Preparers’ websites.”⁸
- f. Assess whether all data transmissions using the Meta Pixel that Mr. Zeidman characterized as “pen register”⁹ data are: (1) necessary for internet communications to occur; and (2) are transmitted or inferred from other transmitted data.

⁶ As discussed in **Section III.E**, I do not offer an opinion on what constitutes sensitive information in this matter, nor did I see any definition of such information provided by Mr. Zeidman or Mr. Weir. Meta defines sensitive data in its terms and policies to include “information defined as sensitive under applicable laws, regulations or industry guidelines, or otherwise not allowed under [Meta’s] terms and policies.” *See, e.g.*, Deposition of Plaintiff Katrina Calderon, (“Calderon Deposition”), May 30, 2025, Exhibit 23 (“About prohibited information[:] At Meta, we have policies around the kinds of information businesses can share with us. We don’t want or permit advertisers to use the Meta Business Tools to share prohibited information about people, which is information defined as sensitive under applicable laws, regulations or industry guidelines, or otherwise not allowed under our terms and policies. This information shouldn’t be shared with us in Meta Business Tools data such as URL parameters, custom event names and custom data. Sharing this type of information in any form goes against the Meta Business Tools Terms and can lead to data restrictions. [...] You must not share any of the following with Meta via the Meta Business Tools: [...] Data that is based on or includes, directly or otherwise, health, financial, consumer report or other categories of sensitive information about people, including information defined as sensitive under applicable laws, regulations and industry guidelines[.]”).

See, e.g., [REDACTED]

⁷ Zeidman Report, ¶ 40.

⁸ Zeidman Report, ¶ 57(2).

⁹ Zeidman Report, ¶ 4.

8. My opinions are set forth in this Rebuttal Report. If I do not address a specific sentence or opinion in the Zeidman Report or the Weir Report, it should not be construed as an implied agreement with those sentences or opinions. My work on this matter is ongoing, and I may update, refine, or revise my opinions, as well as form further opinions, if I review additional materials or conduct further analysis in this matter.

C. Facts and Data Considered

9. In forming my opinions, I reviewed information produced in the litigation, including but not limited to Meta documentation, samples of event data sent from the H&R Block and TaxAct websites to Meta, event data for Sait Kurmangaliyev, Tiffany Bryant, Katrina Calderon, and Jane Doe (the “Named Plaintiffs”),¹⁰ source code, and deposition testimony. I also reviewed information from public sources, including technical documentation from Meta’s website describing the Meta Pixel and Conversions API and sources on how relevant technologies related to modern web communications operate, and conducted my own testing. The sources I relied on to reach my opinions are identified in this report and listed in the attached **Appendix C**.

D. Summary of Plaintiffs’ Allegations

10. I understand plaintiffs have proposed the following classes for certification:

- a. The Nationwide Pen Register Classes:¹¹
 - i. “H&R Block.com: All individuals in the United States who visited the website H&R Block.com from January 15, 2019 to June 30, 2023.”
 - ii. “TaxAct.com: All individuals in the United States who visited the website TaxAct.com from August 25, 2015 to June 30, 2023.”

¹⁰ I assume that the Named Plaintiffs’ event data provided by counsel is complete and correct.

¹¹ *In re Meta Pixel Tax Filing Cases*, Notice of Motion and Motion for Class Certification, Supporting Memorandum of Points and Authorities, Case No. 5:22-cv-07557-PCP, August 18, 2025 (“Motion for Class Certification”), p. i.

- b. The Nationwide Eavesdropping Classes:¹²
 - i. “H&R Block.com: All individuals in the United States who visited the website H&R Block.com from January 15, 2019 to June 30, 2023.”
 - ii. “TaxAct.com: All individuals in the United States who visited the website TaxAct.com from August 25, 2015 to June 30, 2023.”
- c. The California Wiretapping Classes:¹³
 - i. “H&R Block.com: All individuals in California who visited the website H&R Block.com from January 15, 2019 to June 30, 2023.”
 - ii. “TaxAct.com: All individuals in California who visited the website TaxAct.com from August 25, 2015 to June 30, 2023.”
- d. The Nationwide UCL Public Injunctive Relief Classes:¹⁴
 - i. “H&R Block.com: All individuals in the United States who visited the website H&R Block.com from January 15, 2019 to June 30, 2023.”
 - ii. “TaxAct.com: All individuals in the United States who visited the website TaxAct.com from August 25, 2015 to June 30, 2023.”

11. Plaintiffs allege that: “[w]hen users of the tax-filing websites H&R Block and TaxAct accessed the websites to prepare and file their taxes, [Meta] was surreptitiously behind the scenes collecting a wide array of data about those users through its use of its ‘Meta Pixel’ technology.”¹⁵ Plaintiffs categorize that data as:

- a. “*Pen-Register Information*,” which plaintiffs describe as “the date and time [class members] were on the website, their operating system information, browser information, device type information, IP address, and geolocation data.”¹⁶ Plaintiffs alleged that “[t]he Meta Pixel collected this pen register information each time someone visited H&R Block’s and TaxAct’s websites during the proposed class periods”¹⁷ and that “Meta’s filtering systems do not prevent its

¹² Motion for Class Certification, p. i–ii.

¹³ Motion for Class Certification, p. ii.

¹⁴ Motion for Class Certification, p. ii.

¹⁵ Motion for Class Certification, p. 1.

¹⁶ Motion for Class Certification, p. 2.

¹⁷ Motion for Class Certification, p. 2.

ingestion of this information, as shown by the Plaintiffs’ Hive data and the sample Hive data for members of the classes.”¹⁸

- b. “*Contents of Website Visitors’ Communications with Websites*,” which plaintiffs describe as “URL data from H&R Block’s and TaxAct’s websites showing which pages website visitors searched for and visited, ‘thereby divulg[ing] a user’s personal interests, queries, and habits on third-party websites operating outside of Facebook’s platform.’”¹⁹ Plaintiffs allege that “Meta did not attempt to block or filter this type of information until it launched its ‘Core Setup’ program in July 2023.”²⁰
- c. “*Tax Information*,” which plaintiffs describe as “state revenue, number of dependents, tax form, W2, ‘agi’ (adjusted gross income), federal amount owed, and federal refund amounts.”²¹ Plaintiffs allege that “Meta purportedly implemented a filter, ostensibly to attempt to block some financial data[,]” but the filter is unreliable and not designed to filter most of the data at issue here.²²

II. SUMMARY OF OPINIONS

12. I have reached the following opinions based on my review of the information identified herein.

- a. Mr. Zeidman’s and Mr. Weir’s proposed methodologies for counting visits to the H&R Block and Tax Act websites are flawed (**Section IV**).
 - i. Their proposed methodologies are unreliable because (1) Mr. Zeidman’s assumption that each [REDACTED] equates to a website visit is unsupported; and (2) Their proposed methodologies count visits from non-humans (bot traffic), inflating the number of genuine user visits (**Section IV.A**).
 - ii. Their proposed methodologies cannot be used to exclude visits from individuals who consented to cookies (**Section IV.B**).

¹⁸ Motion for Class Certification, p. 3.

¹⁹ Motion for Class Certification, p. 3.

²⁰ Motion for Class Certification, p. 4.

²¹ Motion for Class Certification, p. 4.

²² Motion for Class Certification, p. 5. I also note that this differs from the parameters Mr. Zeidman identified in reference to “tax information,” which include: age range (“age_range”), return year (“return_year”), adjusted gross income (“agi”), federal revenue (“federal_revenue”), federal amount owed (“federal_owe_amount”), federal refund amount (“federal_refund_amount”), number of dependents (“num_of_dependents”), number of standard deductions (“standard_deduction”), state revenue (“state_revenue”), and tax form used (“tax_form”). See Zeidman Report, ¶ 49.

- iii. Their proposed methodologies cannot be used to count visits from individuals in California (**Section IV.C**).
- b. Mr. Zeidman’s and Mr. Weir’s methodologies for counting visits to the H&R Block and Tax Act websites are incapable of accurately identifying visitors to the websites during the proposed class periods (**Section V**).
- c. Mr. Zeidman’s opinion that he found an “enormous” amount of “tax information” and other data transmitted to Meta is unreliable (**Section VI**).
 - i. Mr. Zeidman’s opinions contain significant methodological flaws (**Section VI.A**).
 - ii. My independent review shows that the event data Mr. Zeidman analyzed appears infrequently (**Section VI.B**).
- d. Mr. Zeidman’s claim that “the Meta Pixel operated in a largely uniform manner” across the H&R Block and TaxAct websites during the proposed class periods is wrong. Mr. Zeidman failed to consider variability in the data transmitted as a result of developers’ use of the Meta Pixel, at least due to the following (**Section VII**):
 - i. Mr. Zeidman failed to consider that users have controls that are designed to prevent or limit the transmission of data via the Meta Pixel (**Section VII.A**).
 - ii. Developers, including H&R Block and TaxAct, have controls that limit or modify the data transmitted as a result of their use of the Meta Pixel, and TaxAct and H&R Block used those controls in ways that affected the transmission of data (**Section VII.B**).
 - iii. There was variability in the detection and filtration measures Meta implemented that would have resulted in variability in the types of data Meta received (**Section VII.C**).
- e. Meta implemented a series of technical measures to prevent transmission or limit the use of received data. Users can opt out of Online Behavioral Advertising through industry-standard tools, in which case Meta excludes such data from personalized ad delivery. Additionally, users can manage and disconnect Off-Facebook Activity, further limiting Meta’s ability to associate external data with users’ accounts (**Section VIII**).
- f. Mr. Zeidman mischaracterized the technical nature of the alleged pen register data (**Section IX**).

III. BACKGROUND

13. Modern websites are complex software products developed iteratively. Updates and modifications for those websites can be informed by user behavior and feedback.²³ Developers can rely on a range of analytics and advertising tags or pixels (*e.g.*, Meta Pixel,²⁴ Google Analytics,²⁵ Adobe Analytics,²⁶ and Mixpanel²⁷) to determine which features and functionalities of their websites users value, and to increase the effectiveness of ads by improving the likelihood that they are served to users who find them relevant.²⁸ These analytics and advertising tags or pixels are small snippets of code that developers can embed within their websites.²⁹ The tags or pixels enable developers to implement complex functionalities into their websites without building them from

²³ See, *e.g.*, Quiroz-Vázquez, Camilo, “What Is Software Development?” *IBM*, <https://www.ibm.com/think/topics/software-development>, accessed October 25, 2025 (“Often organizations use preliminary releases, such as beta tests, before releasing a new product to the public. These tests release the product to a selected group of users for testing and feedback and enable teams to identify and address unforeseen issues with the software before a public release.”).

²⁴ See “Meta Pixel,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/>, accessed October 25, 2025. See also, “About Conversions API,” *Meta Business Help Center*, <https://www.facebook.com/business/help/2041148702652965>, accessed July 29, 2025.

²⁵ See “The Finer Points,” *Google Marketing Platform*, <https://marketingplatform.google.com/about/analytics/features>, accessed October 20, 2025. See also, “How Google Analytics Works,” *Google Analytics Help*, <https://support.google.com/analytics/answer/12159447>, accessed September 14, 2025.

²⁶ See “Unified Customer Analytics across Data, Content and Journeys,” *Adobe for Business*, <https://business.adobe.com/products/analytics/adobe-analytics.html>, accessed September 14, 2025.

²⁷ See “Mixpanel Marketing Analytics: From Clicks to Conversions to Revenue,” *Mixpanel*, <https://mixpanel.com/m/mixpanel-marketing-analytics>, accessed September 18, 2025.

²⁸ See, *e.g.*, Higgins, Malcolm, “What Is a Tracking Pixel, and How Does It Work?” *NordVPN*, September 27, 2023, <https://nordvpn.com/blog/what-is-a-tracking-pixel/>, accessed October 25, 2025 (“A tracking pixel can provide its creator with useful information about certain internet users and helps online stores and advertisers assess the effectiveness of various marketing strategies.”).

²⁹ Higgins, Malcolm, “What Is a Tracking Pixel, and How Does It Work?” *NordVPN*, September 27, 2023, <https://nordvpn.com/blog/what-is-a-tracking-pixel/>, accessed October 25, 2025 (“The process of inserting a tracking pixel into digital content is known as embedding or integration.”).

scratch, which may be costly and often impractical.³⁰ Relying on tag or pixel code developed by third parties is standard practice in modern website development.³¹

14. Once a developer integrates pixel code into its website (e.g., LinkedIn Tag Insight or Google Tag), the developer may use the pixel code to transmit certain information to the third-party provider.³² Developers can configure pixel code according to their needs and transmit information they want,³³ as long as it complies with the third-party provider’s terms of service and any technical restrictions the third-party provider has implemented. Developers can use pixel code to transmit “event data,” which is generated when users take actions on the website that developers

³⁰ Higgins, Malcolm, “What Is a Tracking Pixel, and How Does It Work?” *NordVPN*, September 27, 2023, <https://nordvpn.com/blog/what-is-a-tracking-pixel/>, accessed October 25, 2025 (“Companies and websites use tracking pixels to gather data on user behavior, such as their shopping patterns, and optimize their content accordingly. User information helps businesses to work out what the most effective marketing strategies are, making it less likely that they’ll waste money on ineffective ads and email campaigns.”).

³¹ Karlovitch, Sara, “Privacy Tools Fall Short: Here’s What the Numbers Say,” *Marketing Dive*, April 5, 2024, <https://www.marketingdive.com/news/privacy-landscape-increasingly-complex-pixels-what-numbers-say/712387/>, accessed October 25, 2025 (“The report found the widespread use of tracking pixels, which serve a similar purpose to the third-party cookies [...]. Nearly half of all websites (47%) have a Meta pixel, while 12% have a TikTok pixel.”).

³² See, e.g., “LinkedIn Insight Tag FAQs,” *LinkedIn Help*, <https://www.linkedin.com/help/linkedin/answer/a427660>, accessed September 16, 2025 (“The LinkedIn Insight Tag enables the collection of data regarding members’ visits to your website, including the URL, referrer, IP address, device and browser characteristics (User Agent), and timestamp. [...] If you enable enhanced matching, you can also send emails associated with the respective visits. Those emails are hashed on the website before being sent to LinkedIn, [...]”); “About the Google Tag,” *Google Analytics Help*, <https://support.google.com/analytics/answer/11994839>, accessed October 23, 2025 (“The Google tag (gtag.js) is a single tag you can add to your website that allows you to use a variety of Google products and services. [...] The Google tag lets you send data from your website to linked Google product destinations to help you measure the effectiveness of your website and ads.”).

³³ See, e.g., “Configure Your Google Tag Settings,” *Google Analytics Help*, <https://support.google.com/analytics/answer/12131703>, accessed October 23, 2025 (“Tag settings affect the behavior of your Google tag and the data sent to configured destinations. Some settings may be more or less relevant for you depending on which products you use. You may choose to configure settings that are less relevant for your current usage of the Google tag.”); “Manage Your LinkedIn Insight Tag in Campaign Manager,” *LinkedIn Help*, <https://www.linkedin.com/help/lms/answer/a415868>, accessed October 25, 2025 (“To manage the Insight Tag associated with your ad account: [...] You can also click the Manage Insight Tag dropdown: Manage sharing - Manage your Insight Tag sharing. Settings - Enable enhanced conversion tracking. Delete - Delete your Insight Tag.”).

have chosen to log.³⁴ For example, a developer may log an event every time someone makes a purchase on its website. The third-party provider that receives data that the developer sends using the pixel code can then use that data to provide analytics or advertising services to the developer.³⁵

A. The Meta Pixel

1. What the Meta Pixel Is and How It Operates

15. The Meta Pixel is a publicly available, free-to-use snippet of code that developers can copy, customize, and embed in their websites to generate and transmit data points when users take selected actions on their websites and to leverage Meta’s analytics and advertising services.³⁶

³⁴ See, e.g., “Meta Pixel,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/>, accessed July 29, 2025 (“[Meta Pixel] works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion).”); “Introduction to Tagging and the Google Tag,” *Google Tag Platform*, <https://developers.google.com/tag-platform/devguides>, accessed October 25, 2025 (“Tagging is the process of adding snippets of code (called tags) to each page of your website so you can learn about the people who visit your site and how they interact with it [...] Whether you want to know about your most popular blog posts, most effective landing pages, or most popular products, the data you’ll collect through tagging lets you make more informed decisions about your site and your marketing strategies.”).

³⁵ Google and LinkedIn use pixels. See, e.g., “How Google Analytics Work,” *Google Analytics Help*, <https://support.google.com/analytics/answer/12159447>, accessed September 14, 2025 (“Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business. [...] To measure a website, you first have to create a Google Analytics account. Then you need to add a small piece of JavaScript measurement code to each page on your site. Every time a user visits a webpage, the tracking code will collect pseudonymous information about how that user interacted with the page. [...] When the measurement code collects data, it packages that information up and sends it to Google Analytics to be processed into reports. When Analytics processes data, it aggregates and organizes the data [...] Once the data has been processed and stored in the database, it will appear in Google Analytics as reports.”); “LinkedIn Insight Tag FAQs,” *LinkedIn Help*, <https://www.linkedin.com/help/linkedin/answer/a427660>, accessed September 16, 2025 (“The LinkedIn Insight Tag is a piece of lightweight JavaScript code that you can add to your website to enable features like in-depth campaign reporting[.] You can use the LinkedIn Insight Tag to track conversions, retarget website visitors, and learn aggregate insights about categories of members interacting with your ads. [...] The LinkedIn Insight Tag enables the collection of data regarding members’ visits to your website, including the URL, referrer, IP address, device and browser characteristics (User Agent), and timestamp. [...] You can use the LinkedIn Insight Tag to track conversions, retarget website visitors, and learn aggregate insights about categories of members interacting with your ads. [...] If you enable enhanced matching, you can also send emails associated to the respective visits. Those emails are hashed on the website before being sent to LinkedIn, to protect members’ privacy[.]”).

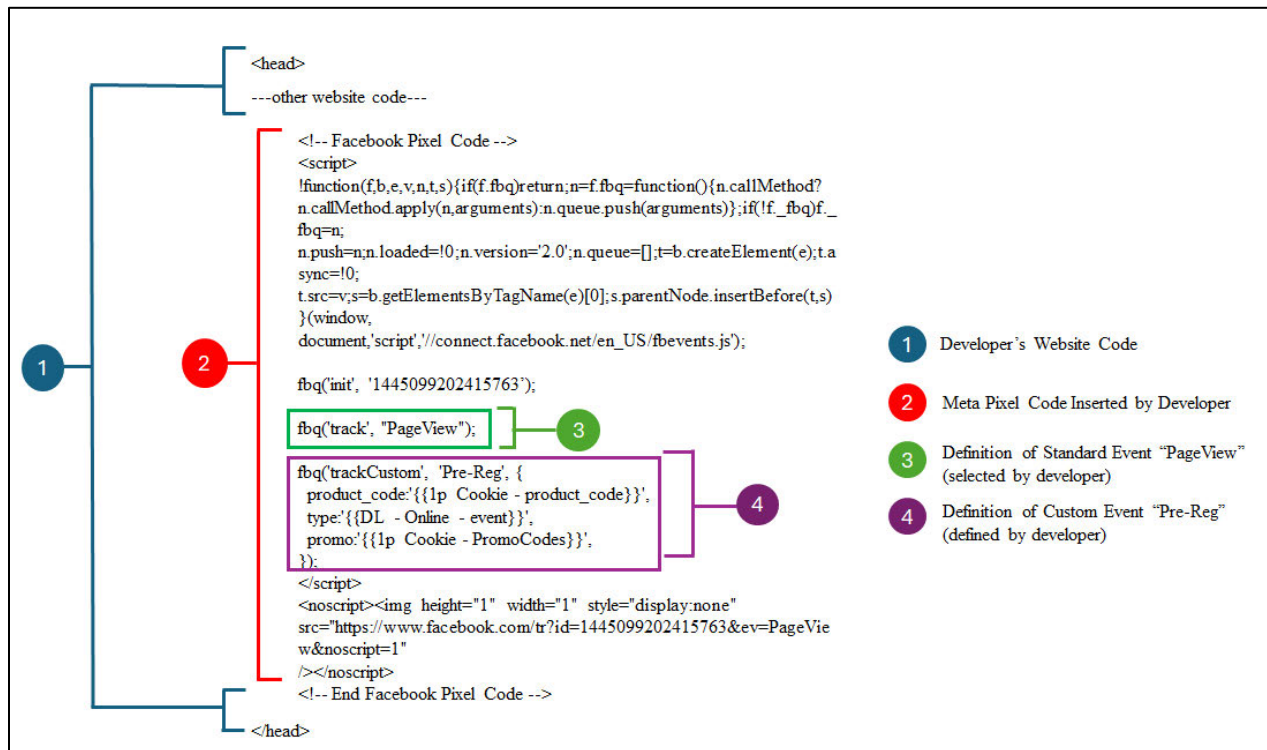
³⁶ “Meta Pixel,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/>, accessed July 29, 2025 (“The Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that [sic] effectiveness of your website’s conversion funnels.”); “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>,

During the process for creating a Meta Pixel ID, developers must agree to Meta’s Business Tools Terms.³⁷ The Meta Pixel operates by first loading JavaScript from the *connect.facebook.net* subdomain to execute the functionalities that developers have configured the Meta Pixel to use (see **Figure 1**).³⁸

accessed October 25, 2025 (“The Pixel’s base code must already be installed on every page where you want to track conversions.”); “Facebook Pixel Events,” *Meta*, <https://www.facebook.com/business/m/one-sheeters/facebook-pixel-events>, accessed October 25, 2025 (“You or your web developer can implement the pixel directly on your website.”); “Facebook Pixel: What It Is and Why You Need It,” *SEO Digital Group*, <https://seodigitalgroup.com/facebook-pixel/>, accessed September 15, 2025 (“Installing the Facebook pixel is totally free.”).

³⁷ “Meta Business Tools Terms,” *Meta*, August 23, 2025, https://www.facebook.com/legal/technology_terms, accessed October 25, 2025 (“Meta Business Tools Terms[:] When you use any of the Meta Business Tools to send us or otherwise enable the collection of Business Tool Data [...], these Business Tools Terms govern the use of that data. [...] We may receive Business Tool Data as a result of your use of Meta ad products, in connection with advertising, matching, measurement and analytics. Those ad products include, but are not limited to, Meta Pixel, [...]. These Business Tools Terms supplement and amend the Commercial Terms of Service.”). *See also*, “Meta Commercial Terms (‘Commercial Terms’),” *Meta*, March 6, 2024, https://www.facebook.com/legal/commercial_terms, accessed October 25, 2025.

³⁸ “Get Started,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/get-started/>, accessed October 25, 2025 (“The Meta Pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. [...] The base pixel code contains your Pixel’s ID in two places and looks like this: [...] s.parentNode.insertBefore(t,s)}(window, document, ‘script’, ‘https://connect.facebook.net/en_US/fbevents.js’).”).

Figure 1: Example of Meta Pixel Code Inserted by Developer into Website Source Code³⁹

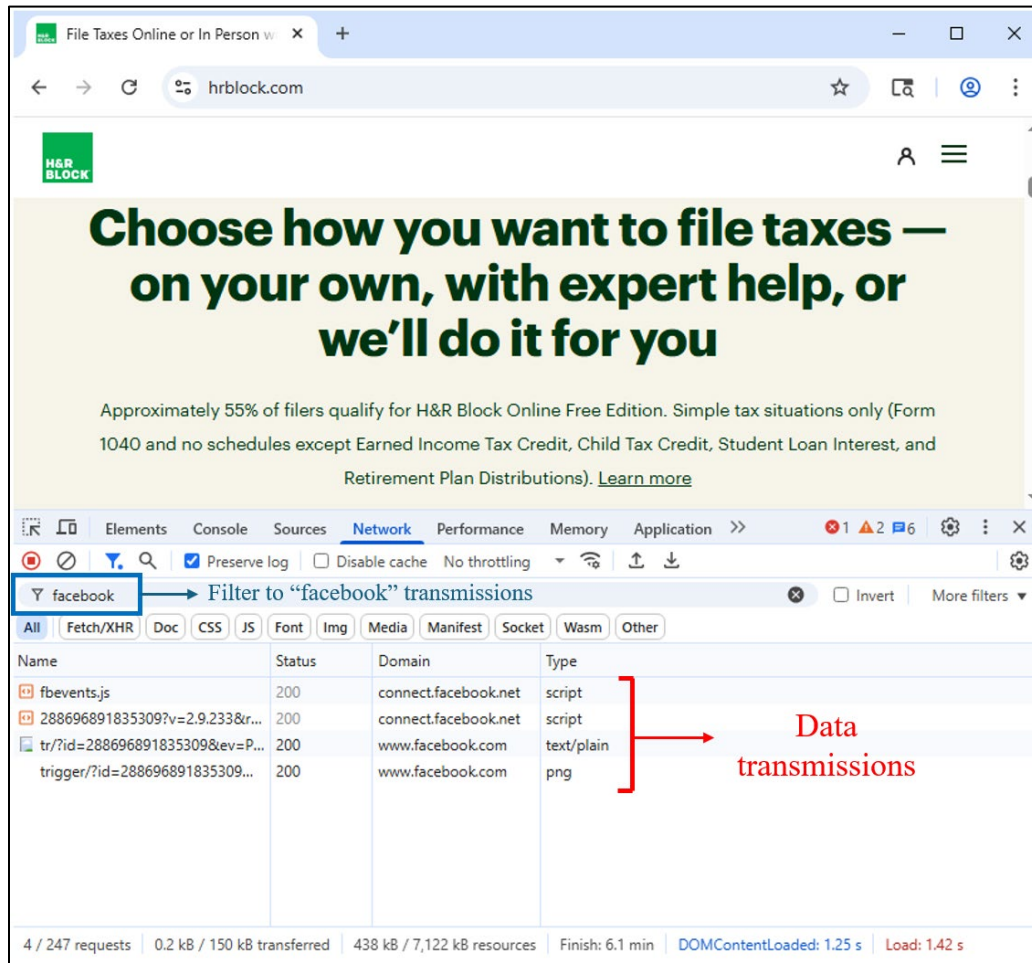
16. Event data might be transmitted from the user's browser to *facebook.com* if a user takes certain actions on a webpage on which a developer has chosen to install the Meta Pixel. However, the data transmitted depends on user and developer controls (see **Sections VII.A** and **VII.B**) in addition to Meta's technical measures (see **Section III.E**), as these controls and measures determine whether or not the Meta Pixel can send specific events associated with those actions.⁴⁰ These data transmissions also include such information as IP addresses, standard HTTP data (e.g.,

³⁹ The snippet of code is an example used by the TaxAct website, as indicated in the tag manager configurations produced in this matter. See TaxAct_00719, line 17477.

⁴⁰ Specifically, transmissions via the Meta Pixel that contain event information, rather than transmissions to *connect.facebook.net* which initiate a connection to Meta servers, are directed to Meta's servers access points at *facebook.com/tr*. See "Specifications for Meta Pixel Standard Events," *Meta Business Help Center*, <https://www.facebook.com/business/help/402791146561655>, accessed September 22, 2025.

headers and cookies),⁴¹ and a Meta Pixel ID. Meta may use the data transmissions to match event data with a Meta user account if possible.⁴² The screenshot of H&R Block’s website in **Figure 2** shows data transmissions resulting from the H&R Block website’s use of the Meta Pixel.⁴³

Figure 2: Meta Pixel Data Transmissions from a Visit to *hrblock.com*⁴⁴



⁴¹ “Meta Pixel,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/>, accessed October 25, 2025 (“The Meta Pixel can collect the following data: Http Headers – Anything that is generally present in HTTP headers, a standard web protocol sent between any browser request and any server on the internet. This information may include data like IP addresses, information about the web browser, page location, document, referrer and person using the website.”).

⁴² See PIXEL_TAX000051247–287 at 254.

⁴³ I discuss and provide support for websites visit tests in **Appendix D** and in my produced backup materials, respectively. The “Testing” directory of my produced backup materials contains the supporting material. For all subsequent tests discussed in my report, I cite the specific folder or file name in my produced backup materials.

⁴⁴ See **Appendix D**; “windows_chrome_hrblock_default.har” in my produced backup materials.

17. Developers can use the Meta Pixel or other analytics pixels to help them learn what website elements users do and do not engage with, such as the pages of their websites that users visit, what buttons they click, or what products they add to a shopping cart.⁴⁵ This may allow developers to, for example, measure the effectiveness of their Facebook and Instagram ads, enabling them to make better decisions about marketing spending.⁴⁶

2. *Event Data Generated by Developers’ Use of the Meta Pixel*

18. Developers can configure the Meta Pixel to create and transmit event data when a user takes an action on their website; these actions are generally referred to as “events.”⁴⁷ Event data is typically composed of an “event name” and a set of optional “event parameters,” sent together in the form of “key-value” pairs.⁴⁸ For example, a developer may configure the Meta Pixel

⁴⁵ “About Meta Pixel,” Meta Business Help Center, <https://www.facebook.com/business/help/742478679120153>, accessed July 29, 2025 (“Once you’ve set up the Meta Pixel, the pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase.”).

⁴⁶ “About Meta Pixel,” Meta Business Help, <https://www.facebook.com/business/help/742478679120153>, accessed July 29, 2025 (“Better understand the impact of your ads by measuring what happens when people see them.”); MacFarlane, Rebecca, “Meta Pixel (Formerly Facebook Pixel): The Ultimate Guide for Marketers,” Sociality.io Blog, July 4, 2023, <https://sociality.io/blog/facebook-pixel/>, accessed September 15, 2025 (“The Meta pixel is a piece of code designed to help you measure the efficacy of your Facebook ad campaigns by monitoring the action(s) users take on your website.”); Altynai Alamanova, “How to Use Facebook Ads for Beginners,” Sociality.io Blog, September 16, 2019, <https://sociality.io/blog/how-to-use-facebook-ads/>, accessed September 15, 2025 (“Facebook offers different kinds of places where your ads can appear.”). The Meta Pixel, however, is not required to run ads with Meta’s advertising services. Developers can still advertise without the Meta Pixel but will not have access to the services and features that it provides. *See also*, Polson, Billy, “Can I Run Facebook Ads Without a Pixel?” *AIDA*, January 1, 2025, <https://aiad.com.au/blog/can-i-run-facebook-ads-without-a-pixel/>, accessed October 14, 2025 (“Facebook allows you to run quite extensive campaigns without requiring the Facebook pixel.”).

⁴⁷ “Specifications for Meta Pixel Standard Events,” *Meta*, <https://www.facebook.com/business/help/402791146561655>, accessed September 22, 2025 (“Events are actions people take on your website.”).

⁴⁸ “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>, accessed October 25, 2025 (“Parameters are optional, JSON-formatted objects that you can include when tracking standard and custom events. They allow you to provide additional information about your website visitors’ actions. [...] You can include the following predefined object properties with any custom events and any standard events that support them. [...] Property Key[,] Value Type”); Jayakumar Deposition, at 91:20–24 (“THE WITNESS: The values represented in the custom data JSON column does represent the key value pairs that’s transmitted as Event Data from the Pixel in a JSON -- stored in a JSON format.”), 178:5–11 (“Q. And Custom Events are -- is the one where website developers can decide whether to include optional parameters; is that correct? A. Developers may choose to include event parameters or key value pairs for all events that they set

so that a user’s purchasing action will generate an event called “purchase,” which could include parameters like “price” and “currency” with values of “20” and “USD,” respectively.⁴⁹ Parameters can be standard or custom. Standard parameters are predefined by Meta, while Custom parameters are created by developers.⁵⁰ In addition to event parameters, data transmissions resulting from developers’ use of the Meta Pixel include the URL from which the Meta Pixel “fired” (*i.e.*, the URL where the user action took place). The URL contains, at a minimum, the domain name (*e.g.*, hrblock.com) and possibly additional elements like a path or query parameters and values, as programmed by website developers.

19. In general, developers have a range of controls to configure the Meta Pixel to determine what events and parameters to generate and transmit to Meta, when they are sent, for what users, and from which webpages. Over time, developers can change what event data to generate and transmit to Meta, when those events “fire,” for what users, and from which webpages. Thus, Meta may receive certain event data for some visitors to their websites but not for others. As I explain in **Section VII.B**, both H&R Block and TaxAct made use of these developer controls.

up, including standard convenience as well.”). *See also*, Erickson, Jeffrey, “What Is JSON,” *Oracle*, April 4, 2024, <https://www.oracle.com/database/what-is-json/>, accessed October 25, 2025; “Parameters,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters>, accessed October 25, 2025.

⁴⁹ *See* “Set the Value and Currency of Your Meta Pixel Standard Events,” *Meta Business Help Center*, <https://www.facebook.com/business/help/392174274295227>, accessed October 20, 2025.

⁵⁰ “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>, accessed October 25, 2025 (“Parameters are optional, JSON-formatted objects that you can include when tracking standard and custom events. They allow you to provide additional information about your website visitors’ actions.”); “Standard Parameters,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/custom-data>, accessed October 26, 2025 (“This table lists all standard parameters users can send to Meta. Website Standard Parameters[,] App Standard Parameters[,] Offline Standard Parameters”). *See also*, “Reference,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/reference/>, accessed October 23, 2025.

20. The developer can configure the Meta Pixel to generate three types of events: (1) Standard Events, (2) Automatic Events, and (3) Custom Events.⁵¹

21. **Standard Events** are “actions with predefined names that Meta recognizes and supports” across its Business Tools, such as Meta Pixel and CAPI (*e.g.*, “AddToCart,” “Donate,” “Lead”).⁵² Although these events have names predefined by Meta, Standard Events are not transmitted by default, and developers must use code to set up the Meta Pixel to use them.⁵³ Developers can configure the Meta Pixel according to their needs and may use Standard Events in ways that work best for them. As such, a Standard Event name may not describe the user action for which event data were generated.⁵⁴ For example, although Meta’s description of the Standard Event

⁵¹ “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/>, accessed October 26, 2025 (“If [Meta’s] predefined standard events aren’t suitable for [developers’] needs, [they] can track [their] own custom events, which also can be used to define custom audiences for ad optimization. Custom events also support parameters, which [developers] can include to provide additional information about each custom event.”).

⁵² “About Standard and Custom Website Events,” *Meta Business Help Center*, <https://www.facebook.com/business/help/964258670337005>, accessed October 7, 2025 (“Standard events: These are actions with predefined names that Meta recognizes and support across ad product. [Developers] can set up standard events using the event setup tool, a partner integration, [developer’s website] pixel code, or Conversions API code.”); “Specifications for Meta Pixel Standard Events,” *Meta*, <https://www.facebook.com/business/help/402791146561655>, accessed September 22, 2025 (“Standard events[:] [...] Add to cart, [...] Donate, [...] Lead, [...]. The page view event is included as part of [developer’s website] pixel base code.”).

⁵³ Deposition of Amlesh Jayakumar, (“Jayakumar Deposition”), July 14, 2025, at 177:11–17 (“Q. Is it correct to say that Standard Events are predefined by Meta but must be actively added by a website developer? A. Standard events are predefined by Meta, but they need to be actively configured. However that applies to all Event Data that needs to be set up by the Pixel -- set up on the Pixel.”). I note that “PageView,” although a standard event, is included as part of the pixel base code by default. PageView can be turned off by the developer. *See* “Specifications for Meta Pixel Standard Events,” *Meta*, <https://www.facebook.com/business/help/402791146561655>, accessed September 22, 2025 (“The page view event is included as part of [developer website’s] pixel base code.”).

⁵⁴ Mr. Jayakumar testified that Meta cannot interpret event names or parameters or know whether they reflect the actual action taken. *See* Jayakumar Deposition, at 57:8–58:8 (“Q. So Meta has an understanding of what terms like event name means but has no idea what state_revenue, number of dependents, number of child buttons, return year, tax form, has no idea of what any of that stuff means? THE WITNESS: Meta has an understanding of what it should represent, such as the name of the event that’s configured to be sent along the Event Data. By definition, Meta understands what those fields represent. However, even in the case of fields such as Event Name, Meta cannot and doesn’t further interpret what the name of that event, particular event, may represent, such as an action they may or may not have taken on the website. Meta has documentation for certain standard fields, such as Standard Events, that we have public documentation for and recommended certain scenarios. But even then, Meta cannot know for sure what those actions relating to that event may represent.”).

“Contact” is “[w]hen a person initiates contact with your business via telephone, SMS, email, chat, etc.,” it could be implemented to be triggered when a purchase occurs.⁵⁵

22. **Automatic Events** are automatically generated when a developer chooses to install the Meta Pixel on a webpage and users take certain actions on that webpage, without the developers adding any additional code.⁵⁶ These events transmit button clicks and page metadata information.⁵⁷ Developers can turn Automatic Events off.⁵⁸ Whether particular user actions will result in generating and transmitting Automatic Event data depends on how developers configure the Meta Pixel.

23. **Custom Events** are developer-named and -defined to represent an action not captured by Standard Events.⁵⁹ As with Standard Events, developers also decide whether to include

⁵⁵ See, e.g., “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>, accessed October 25, 2025.

⁵⁶ See, e.g., “Set up Automatic Events in Meta Events Manager,” *Meta Business Help Center*, <https://www.facebook.com/business/help/555177831677798>, accessed July 31, 2025 (“Automatic events are events that the Meta Pixel tries to detect automatically on your website. If we’ve detected an event on your website that you may want to start optimizing for, like leads or purchases, then you’ll see a notification in Meta Events Manager.”); “About Automatic Events,” *Meta Business Help Center*, <https://www.facebook.com/business/help/1292598407460746>, accessed July 31, 2025 (“Automatic events are actions that your pixel receives from your website that don’t require you to add any additional code.”).

⁵⁷ “Advanced,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/advanced/>, accessed September 29, 2025 (“The Meta Pixel will send button click and page metadata (such as data structured according to Opengraph or Schema.org formats) from your website to improve your ads delivery and measurement and automate your Pixel setup.”).

⁵⁸ See, e.g., Jayakumar Deposition, at 176:14–22 (“Q. [...] Automatic Events are automatically detected by Meta unless the developer disables logging of Automatic Events; is that correct? A. Automatic Events are those that, if the Pixel is configured to send these events, is sent by Meta for the purposes of making the setup of future Pixel events easier, and can be configured by the developer to not be sent to Meta.”); “Set Up Automatic Events in Meta Events Manager,” *Meta Business Help Center*, <https://www.facebook.com/business/help/555177831677798>, accessed July 31, 2025 (“To turn automatic events on or off: [...] Click to toggle ON or OFF the Track events automatically without code feature under Event setup.”). See also “Advanced,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/advanced/>, accessed September 29, 2025 (“To configure the Meta Pixel to not send this additional information, in the Meta Pixel Base code, add fbq(‘set’, ‘autoConfig’, ‘false’, ‘FB_PIXEL_ID’) above the init call.”).

⁵⁹ “About Standard and Custom Website Events,” *Meta Business Help Center*, <https://www.facebook.com/business/help/964258670337005>, accessed October 7, 2025 (“Custom events: These are actions not covered by standard events. You can assign a unique name to represent the action.”).

optional parameters with Custom Events.⁶⁰ Developers decide how to name Custom Events they decide to define, subject to certain technical restrictions (e.g., character count),⁶¹ and can also choose when these events “fire.”

B. Cookies

24. Cookies, small files stored in browser memory and used by websites to remember certain information about users, play a role in developers’ transmission of data via the Meta Pixel.⁶² Cookies are transmitted via HTTP “Cookie” headers or are set by JavaScript.^{63, 64} Cookies can store a variety of information, including session identifiers, user preferences, and metadata about interactions with the website.⁶⁵ Developers can choose to share cookie values with third parties via

⁶⁰ “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-events>, accessed October 22, 2025 (“Custom events also support parameters, which you can include to provide additional information about each custom event.”).

⁶¹ “Conversion Tracking,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>, accessed October 25, 2025 (“You can track custom events by calling the Pixel’s fbq(‘trackCustom’) function, with your custom event name and (optionally) a JSON object as its parameters. [...] Custom event names must be strings, and cannot exceed 50 characters in length.”).

⁶² “What Are Internet Cookies?,” *Microsoft*, April 25, 2023, <https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies>, accessed September 15, 2025 (“Cookies are bits of data that are sent to and from your browser to identify you. When you open a website, your browser sends a piece of data to the web server hosting that website. This data usually appears as strings of numbers and letters in a text file. Every time you access a new website, a cookie is created and placed in a temporary folder on your device. From here, cookies try to match your preferences for what you want to read, see or purchase.”). *See also*, “ClickID and the fbp and fbc Parameters,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/>, accessed September 15, 2025 (“When the Meta Pixel is installed on a website, and the Pixel uses first-party cookies, the Pixel automatically saves a unique identifier to an fbp cookie for the website domain if one does not already exist. The fbp event parameter value must be of the form version.subdomainIndex.creationTime.randomnumber[.]”).

⁶³ “What Are Third-Party Cookies?,” *Google Privacy Sandbox*, <https://privacysandbox.google.com/cookies/basics/third-party-cookies>, accessed September 15, 2025 (“A cookie is a name and a value communicated using HTTP headers[.]”). *See also*, “Cookie Header,” *Mozilla Developer Network*, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cookie>, accessed September 22, 2025 (“The HTTP Cookie request header contains stored HTTP cookies associated with the server[.]”).

⁶⁴ Cookies can also be set with JavaScript code. “JavaScript Cookies,” *W3Schools*, https://www.w3schools.com/js/js_cookies.asp, accessed October 23, 2025 (“JavaScript can create, read, and delete cookies with the document.cookie property.”).

⁶⁵ Cookie values are not necessarily user identifiers and may contain other types of information, (e.g., “EN” for English). For instance, if several websites use a cookie named “lang” with the value “EN,” that cookie may appear identical across websites but would be independently created and managed by each individual domain.

URL parameters.⁶⁶ Cookies can be first-party—*i.e.*, created and accessed by the website the user is visiting (the “first party”), or they can be third-party—*i.e.*, created and accessed by a domain other than the one the user is visiting (the “third party”).⁶⁷

25. **First-party cookies:** A cookie operates in a first-party context when its domain matches the domain the user is visiting.⁶⁸ First-party cookies are typically used for site-specific functionality, like remembering items in a user’s shopping cart. For example, when a user visits the H&R Block website with cookies enabled in their browser, the website places cookies that it can later access and reuse (*e.g.*, to remember the user’s login information or language preference). Because first-party cookies can only be accessed by the site the user is visiting, they cannot be used alone to track users across different websites.

26. **Third-party cookies:** A cookie operates in a third-party context when it is set or accessed by a domain other than the one the user is visiting.⁶⁹ For example, from the perspective of someone visiting *hrblock.com*, *facebook.com* is a third-party domain. The *facebook.com* domain

“Using HTTP Cookies,” *Mozilla Developer Network*, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies>, accessed September 23, 2025 (“Session management: User sign-in status, shopping cart contents, game scores, or any other user session-related details that the server needs to remember. [...] Personalization: User preferences such as display language and UI theme.”).

⁶⁶ “Using HTTP Cookies,” *Mozilla Developer Network*, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies>, accessed September 23, 2025 (“Define where cookies are sent[:] The Domain and Path attributes define the scope of a cookie: what URLs the cookies are sent to. The Domain attribute specifies which server can receive a cookie. If specified, cookies are available on the specified server and its subdomains. For example, if you set Domain=mozilla.org from mozilla.org, cookies are available on that domain and subdomains like developer.mozilla.org.”).

⁶⁷ Jayakumar Deposition, at 24:10–19 (“Q. What is the distinction between a first-party and a third-party cookie [...]? A. A first-party cookie generally refers to cookies that are set within the context of the domain or the browser, the website, where an action may take place. Whereas, a third-party cookie is set within the context of [...] a domain other than the domain that the user may have visited in the third-party sense.”).

⁶⁸ Merewood, Rowan, “Understanding Cookies,” *web.dev*, October 30, 2019, <https://web.dev/articles/understanding-cookies>, accessed October 25, 2025 (“Cookies that match the domain of the current site, that is, what’s displayed in the browser’s address bar, are referred to as first-party cookies.”).

⁶⁹ Merewood, Rowan, “Understanding Cookies,” *web.dev*, October 30, 2019, <https://web.dev/articles/understanding-cookies>, accessed October 25, 2025 (“Similarly, cookies from domains other than the current site are referred to as third-party cookies. This [...] is relative to the user’s context; the same cookie can be either first-party or third-party depending on which site the user is on at the time.”).

may set a cookie on a user’s browser when that user visits *hrblock.com*. Examples of cookies associated with the *facebook.com* domain include the *c_user*,⁷⁰ *datr*,⁷¹ and *fr* cookies.⁷² Even if a cookie was set in a first-party context, it can be accessed in a third-party context when a site makes an HTTP request to that cookie’s domain.

27. Whether cookies are created and transmitted may vary depending on the user’s browser and the user’s cookie choices. Users can block the transmission of third-party cookies (including those associated with the *facebook.com* domain)—or all cookies—through browser cookie settings, as discussed in **Section VII.A.4** below. As a result, Meta may receive third-party cookie data for some visitors to the H&R Block and TaxAct websites, but not for others.

C. Tag Managers and Consent Management Platforms

28. Developers can use a tag manager to add pixels or tags to their websites. Tag managers are third-party services that allow developers to manage and deploy third-party business tools—such as the Meta Pixel or Google Analytics—on their websites without directly modifying

⁷⁰ The *c_user* cookie is transmitted to Meta only when the user is logged into their Facebook user account. Its value corresponds to the user’s Facebook account ID, which is also visible in the URL during login. *See* “Meta Cookies Policy,” *Meta*, [https://www.facebook.com/privacy/policies/cookies?annotations\[0\]=explanation%2F1_common_cookies_and_us](https://www.facebook.com/privacy/policies/cookies?annotations[0]=explanation%2F1_common_cookies_and_us), accessed October 25, 2025 (“We use these cookies to authenticate you and keep you logged in as you navigate between Facebook Pages.”).

⁷¹ The *datr* cookie is a browser-unique identifier that Meta describes as a security measure, used to recognize trusted browsers where users have previously logged in. *See* “Security, Site and Product Integrity,” *Meta*, https://www.facebook.com/privacy/policies/cookies/version/cookie_policy_2022/?subpage=subpage-1.2, accessed September 15, 2025 (“‘Datr’ is a unique identifier for your browser that, amongst other things, helps us protect you from fraud. For example, it helps us identify trusted browsers where you have logged in before. ‘Datr’ has a lifespan of two years.”).

⁷² The *fr* cookie is used to deliver, measure, and improve the relevancy of ads. *See* “Advertising, Recommendations, Insights and Measurement,” *Meta*, <https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>, accessed September 15, 2025 (“Cookies allow us to help deliver ads to people who have previously visited a business’s website, purchased its products or used its apps and to recommend products and services based on that activity. Cookies also allow us to limit the number of times that you see an ad so you don’t see the same ad over and over again. For example, the ‘fr’ cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.”).

the website’s source code.⁷³ Instead, developers place a container⁷⁴ (e.g., from Google Tag Manager or Adobe Tag Manager) in the website’s code and then manage additional tags, such as pixel code, through the tag manager interface.

29. Developers can also use Consent Management Platforms (“CMPs”), either standalone or as part of a tag manager,⁷⁵ to allow users to enable or disable pixel functionality.⁷⁶ For example, OneTrust is a CMP that helps manage consent preferences by “set[ting] up consent interfaces based on location, regulation, and industry.”⁷⁷ For example, users who are presented with

⁷³ See, e.g., “About Google Tag Manager,” *Google Tag Platform*, <https://developers.google.com/tag-platform/tag-manager>, accessed October 14, 2025 (“Use [Google] Tag Manager to manage tags (such as measurement and marketing optimization JavaScript tags) on your site. Without editing your site code, use Tag Manager to add and update Google Ads, Google Analytics, Floodlight, and third-party tags.”); “Add the Meta Pixel with Google Tag Manager,” *Meta Business Help Center*, <https://www.facebook.com/business/help/1021909254506499/>, accessed September 22, 2025 (“Use Google Tag Manager to add your Meta Pixel and optimize advertising results.”).

⁷⁴ A container allows all advertising, analytics, and third-party integrations to be managed collectively, rather than relying on multiple independently implemented tags. See, e.g., “Container,” *Google Tag Manager Help*, <https://support.google.com/tagmanager/answer/12811176>, accessed October 20, 2025 (“A container consists of multiple tags and rules to govern them. There are specific container types that may be used for: Websites[,] AMP pages[,] Android apps[,] iOS apps[,] Running Tag Manager on a server[.]”); “Introduction to Tag Manager,” *Google Tag Manager Help*, <https://support.google.com/tagmanager/answer/6102821>, accessed September 22, 2025 (“A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a container. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.”); “Tag Management,” *Adobe for Business*, <https://business.adobe.com/products/analytics/tag-management.html>, accessed September 22, 2025 (“Launch is our next-generation tag management system that unifies our entire marketing technology ecosystem. With Launch, third-party developers can build, maintain, and continuously update their integrations with Adobe Experience Cloud, meaning you can deploy both Adobe and third-party apps with ease — and capture and use customer data as you please.”).

⁷⁵ “Set Up and Manage Consent - Obtain User Consent,” *Google Tag Manager Help*, <https://support.google.com/tagmanager/answer/14009343>, accessed October 25, 2025 (“Obtain user consent on your website [...] When a user visits your website, you need to ask them for consent so that the Google tag can write and read cookies. To simplify the process of setting up a consent banner, Google partners with consent management platforms. You can also build a consent banner yourself, if your organization requires it.”).

⁷⁶ “Using Meta Pixel with Cookie Consent,” *OneTrust*, July 25, 2025, https://my.onetrust.com/s/article/UUID-dddb471b-4ba0-9710-db93-942700a51cef?language=en_US, accessed October 8, 2025 (“If your organization has implemented the Meta Pixel on its sites to track site visitors or dynamically load advertising content, you will need to ensure your banner script is capable of selectively allowing and disallowing functionality based on site visitor consent preferences.”).

⁷⁷ “Consent & Preferences,” *OneTrust*, <https://www.onetrust.com/solutions/consent-and-preferences/>, accessed October 20, 2025 (“Comply with regional and industry-specific regulations[:] Set up consent interfaces based on location, regulation, and industry. Customize user experiences and options from pre-built templates and configurations. Continuously update your deployment based on regulatory changes.”).

a consent banner when they visit a website, may block data transmissions via the Meta Pixel , as discussed in **Section VII.A.2** below.⁷⁸ The functionality of consent banners (*e.g.*, opt-in vs. opt-out configurations) varies from website to website, geographically (*e.g.*, whether a user IP address is associated with California),⁷⁹ and over time (see **Section VII.A.2**), based on how each developer sets its consent banner.

D. Conversions API

30. An API, or application programming interface, is a set of rules that allows different software systems to communicate with one another.⁸⁰ For example, when someone opens the weather app on their phone, the app may not store all the weather data on the user’s device. Instead, it may send a request through an API to a weather-service server, which responds with the information—such as temperature, precipitation, and wind speed—and the API delivers these data back to the app for display.⁸¹ In short, an API allows one program to interact with a server in a

⁷⁸ As further discussed in **Section VII.A.2**, I also note that developers can implement consent banners independently or with a tag manager. Developers may also adjust the Meta Pixel to configure it to pause transmissions until they indicate consent has been granted. See “General Data Protection Regulation,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/implementation/gdpr/>, accessed October 25, 2025 (“Use the following API to pause sending Pixel fires to Facebook, and once cookie consent is granted, send Pixel fires to Facebook. You need to call revoke on every page.”).

⁷⁹ Zey, Tyler, “How to Run Cookie Banners Only in Certain States (and Hide Them Everywhere Else),” *Ours Privacy*, September 5, 2025, <https://oursprivacy.com/guides/auto-show-cookie-banner-on-region>, accessed October 23, 2025 (“We’ll build a cookie banner with two distinct behaviors: In California (CA): Shows the cookie banner, typically requires users to opt-in, and can disable page interaction until consent is given[.] All Other States: Hides the cookie banner by default (users can open it via a footer link) and defaults to opt-out mode.”).

⁸⁰ Goodwin, Michael, “What Is an API (Application Programming Interface)?,” *IBM*, April 9, 2024, <https://www.ibm.com/think/topics/api>, accessed September 15, 2025 (“An API, or application programming interface, is a set of rules or protocols that enables software applications to communicate with each other to exchange data, features and functionality. [...] APIs are predefined interfaces that share only the necessary data and functions for specific queries. Servers do not have to fully expose data—APIs enable the sharing of small packets of data, relevant to the specific request.”).

⁸¹ “API Web Service,” *National Weather Service*, <https://www.weather.gov/documentation/services-web-api>, accessed September 15, 2025 (“The National Weather Service (NWS) API allows developers access to critical forecasts, alerts, and observations, along with other weather data.”); Eldridge, Thomas, “What Is a Weather API?,” *Meteomatics*, November 13, 2023, <https://www.meteomatics.com/en/weather-api/what-is-a-weather-api/>, accessed September 15, 2025 (“A weather API (Application Programming Interface) is a set of protocols and

defined format, and that server to respond in that same format, facilitating the exchange of data between apps, websites, or services.

31. Conversions API (“CAPI”), also known as Facebook Server-Side API,⁸² is a tool that allows developers to create a direct connection between marketing data stored on their or a third-party cloud provider’s servers and Meta’s systems.⁸³ Developers can use CAPI independently of the Meta Pixel.⁸⁴

32. The data developers choose to send via CAPI comes directly from the developer (*e.g.* a developer’s server) rather than the user’s browser as is the case with the Meta Pixel.⁸⁵ Developers must configure CAPI and choose the names and parameters of the events they wish to transmit. As with the Meta Pixel, the names and parameters of these events may not describe the user actions associated with them.

33. There are differences in how event data is transmitted to Meta’s servers when using the Meta Pixel versus CAPI. When developers configure the Meta Pixel, the event data is generated

tools that allow for the retrieval of weather data from various sources. It acts as an intermediary, enabling software applications to access real-time, forecasted, and historical weather information.”).

⁸² “Meta Pixel and Conversions API,” *Apptrian LLC*, <https://commercemarketplace.adobe.com/apptrian-meta-pixel-and-conversions-api.html>, accessed September 16, 2025 (“The Meta Conversions API (Facebook Conversions API / Facebook Server-Side API) (for web) allows advertisers to send web events from their servers directly to Meta (Facebook). Server-side events are linked to a pixel and are processed like browser pixel events. This means that server-side events are used in measurement, reporting, and optimization in the same way as browser pixel events.”).

⁸³ “About Conversions API,” *Meta Business Help Center*, <https://www.facebook.com/business/help/2041148702652965>, accessed July 29, 2025 (“The Conversions API is designed to create a direct connection between your marketing data and Meta’s ad optimization systems[.]”).

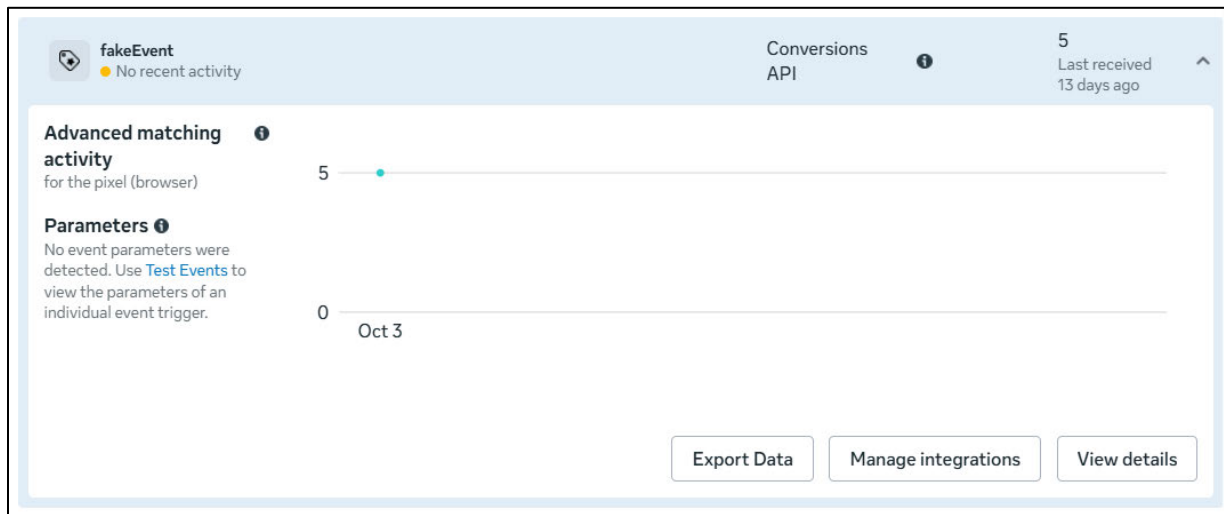
⁸⁴ “Conversions API End-to-End Implementation,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/guides/end-to-end-implementation>, accessed October 25, 2025 (“Data Control: When used via a Server-Only implementation (for example, without the Meta Pixel), the Conversions API gives you added control over what data you share. You can choose to append insights to your events, providing data such as product margins or historical information, like customer value scores.”).

⁸⁵ “Conversions API,” *Meta*, <https://www.facebook.com/business/tools/conversions-api>, accessed September 22, 2025 (“How is the Conversions API different from the Meta Pixel? While both provide the capability to gather and distribute customer data for targeted advertising, optimizing, and measuring ad campaigns, the Conversions API shares data directly from [developers] servers. This can be more reliable than the pixel, which depends on third-party cookies and other data transmitted through web browser protocols.”).

and transmitted to Meta when a user takes an action on their website, (subject to user and browser controls as discussed in **Section VII.A**). With CAPI, developers can transmit event data whenever they want to up to seven days after the event data was generated.⁸⁶ When events are transmitted to Meta can vary from website-to-website, depending on whether a developer uses the Meta Pixel, CAPI, or both. I was able to transmit the Custom Event “fakeEvent” directly to Meta’s servers using CAPI.⁸⁷ I observed that after transmission, the event was displayed in the Meta Events Manager with the associated “event_time” value transmitted (see **Figure 3**).

⁸⁶ Events transmitted with timestamps prior to this period will not be accepted by Meta’s servers. Nonetheless, developers may configure any timestamp with the event they are transmitting and hence can choose to apply a valid timestamp to events that had actually occurred earlier than a week prior to transmission or events that had never occurred. *See* “Using the API,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/using-the-api/>, accessed October 20, 2025 (“event_time is the event transaction time. It should be sent as a Unix timestamp in seconds indicating when the actual event occurred. The specified time may be earlier than the time you send the event to Facebook. This is to enable batch processing and server performance optimization. The event_time can be up to 7 days before you send an event to Meta. If any event_time in data is greater than 7 days in the past, we return an error for the entire request and process no events. For offline and physical store events with physical_store as action_source, you should upload transactions within 62 days of the conversion.”).

⁸⁷ *See Appendix D*; “CAPI Testing” in my produced backup materials.

Figure 3: Custom Event “fakeEvent” in the Meta Events Manager⁸⁸

E. Meta’s Technical Measures

34. Meta prohibits the transmission of sensitive information⁸⁹ from developers that use the Meta Business Tools and has implemented a series of technical measures in an effort to limit or prevent the transmission, receipt, and use of potentially sensitive data.⁹⁰ These technical measures

⁸⁸ I obtained this snapshot from the Meta Event’s manager, which is not publicly available and requires access to the advertising account associated with the transmitted events. Such a dashboard is accessible to anyone with access to Event Manager after creating an account. See “Set Up and Install the Meta Pixel,” *Meta Business Help Center*, <https://www.facebook.com/business/help/952192354843755>, accessed October 26, 2025.

⁸⁹ “Meta Business Tools Terms,” *Meta*, August 23, 2025, https://www.facebook.com/legal/technology_terms, accessed October 25, 2025 (“You represent and warrant that you will not share Business Tool Data with us that you know or reasonably should know is from or about children under the age of 13 or that includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).”).

⁹⁰ I do not offer an opinion on what constitutes sensitive information in this matter, nor did I see any definition of such information provided by Mr. Zeidman or Mr. Weir. Meta defines sensitive data in its terms and policies to include “information defined as sensitive under applicable laws, regulations or industry guidelines, or otherwise not allowed under [Meta’s] terms and policies.” See, e.g., Deposition of Plaintiff Katrina Calderon, (“Calderon Deposition”), May 30, 2025, Exhibit 23 (“About prohibited information[:]. At Meta, we have policies around the kinds of information businesses can share with us. We don’t want or permit advertisers to use the Meta Business Tools to share prohibited information about people, which is information defined as sensitive under applicable laws, regulations or industry guidelines, or otherwise not allowed under our terms and policies. This information shouldn’t be shared with us in Meta Business Tools data such as URL parameters, custom event names and custom data. Sharing this type of information in any form goes against the Meta Business Tools Terms and can lead to data restrictions. [...] You must not share any of the following with Meta via the Meta Business Tools: [...] Data that is based on or includes, directly or otherwise, health, financial, consumer report or other categories

include systems designed to detect and filter potentially sensitive data (**Section III.E.1**) and systems designed to prevent the transmission of certain types of information from certain developers (**Section III.E.2**). Meta also sends notifications to developers when its systems detect and filter potentially sensitive data (**Section III.E.3**). I explain my methodology and analysis of the code Meta produced in this matter in **Appendix D**.

I. Detection and Filtration

35. Meta has developed and continues to maintain integrity systems designed to detect potentially sensitive data, including potentially sensitive financial data.⁹¹ According to Meta’s technical documentation and code I reviewed, Meta’s systems maintain information about the source (*e.g.*, Pixel ID) and the keys associated with any potentially sensitive data identified through the detection systems (see **Figure 4**).⁹² That information is subsequently used to detect and filter out those potentially sensitive keys from future events from that source, prior to storing any remaining data.⁹³

of sensitive information about people, including information defined as sensitive under applicable laws, regulations and industry guidelines[.]”).

See, e.g., [REDACTED]

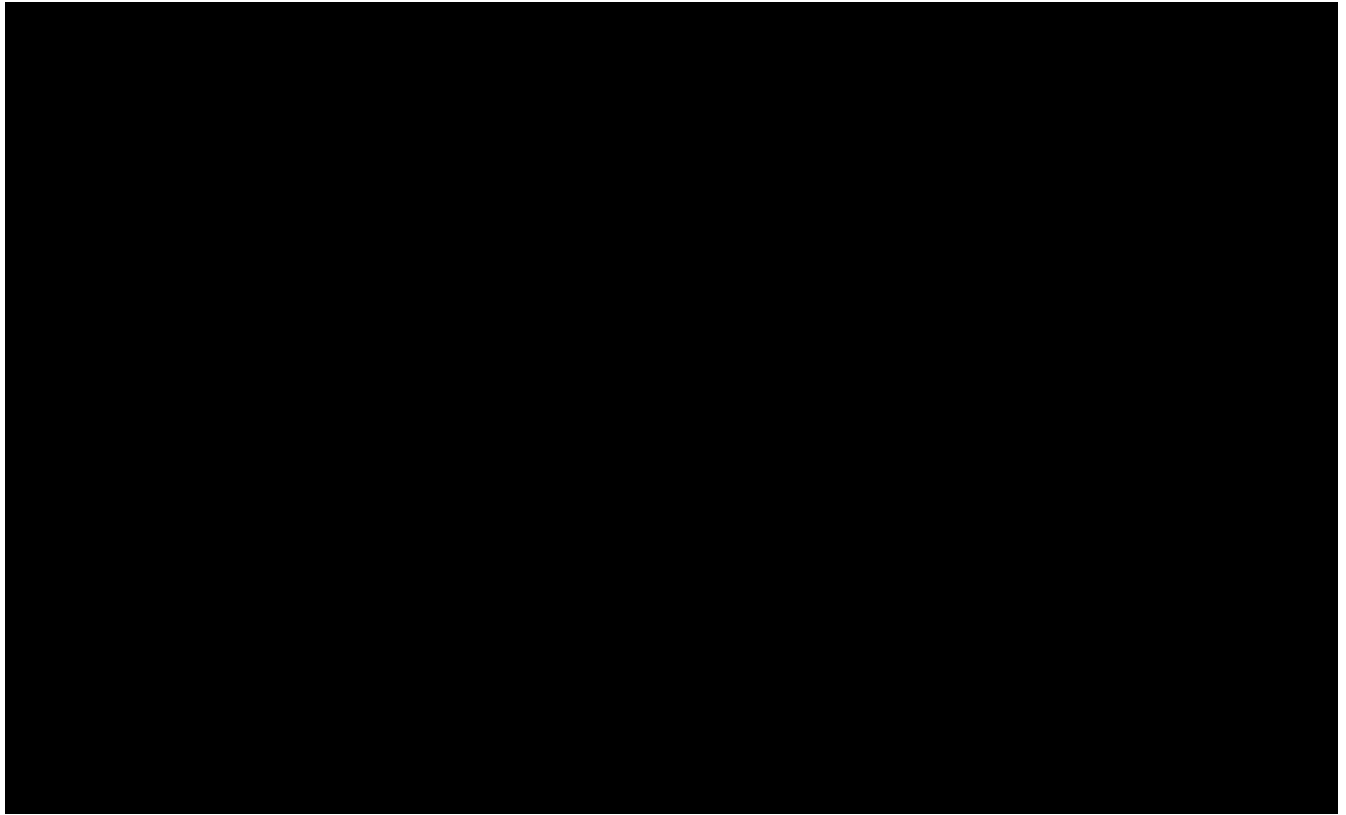
⁹¹ Meta refers to a range of systems designed to filter out potentially sensitive data detected by Meta before it is stored and used in Meta’s system as “integrity” or “signals integrity” systems. *See, e.g.,* [REDACTED]

⁹² PIXEL TAX000057424-426 at 424 [REDACTED]

See also [REDACTED]

⁹³ *See, e.g.,* [REDACTED]

Highly Confidential – Attorneys’ Eyes Only



a) Universal Integrity System

36. In October 2018, Meta implemented a “universal filtering” integrity system.⁹⁵ This system is designed to apply to certain event data, [REDACTED]

[REDACTED]

⁹⁴ [REDACTED] See PIXEL_TAX000057424-426 at 424.

⁹⁵ See, e.g., [REDACTED]

PIXEL TAX000057427-429 at 427 [REDACTED]

data.⁹⁶

⁹⁷ Meta's measures have evolved over time,

in July 2019.⁹⁸ In early 2023, Meta added

⁹⁶ See, e.g., [REDACTED]

recognizable patterns. For example, [REDACTED]

(“DETECTION STRATEGIES[:] We have the following detection strategies currently implemented in

PIXEL TAX000057427-429 at 427

98 [REDACTED]

99

38. In addition to the rules described above, the universal filtration system was [REDACTED]
[REDACTED] Meta included a detector based on a
[REDACTED] in March 2019.¹⁰⁰ Meta added the [REDACTED]
[REDACTED], in September 2019.¹⁰¹

b) The Finance Filter

39. In late 2021, Meta launched an enhanced finance-specific integrity system for
Business Tools (e.g., the Meta Pixel and CAPI) that applies to [REDACTED]

99

100

See also PIXEL TAX000057424-426 at 425

101

See also PIXEL TAX000057427-429 at 427

[REDACTED]

[REDACTED]¹⁰² The finance filtration system uses [REDACTED]

[REDACTED]—to filter out potentially sensitive financial information that it is able to detect. The types of information that this filter is designed to detect include, but are not limited to: [REDACTED]

[REDACTED].¹⁰³ Meta has continued developing the functionality of the financial filtering system over time.¹⁰⁴

102

[REDACTED]

[REDACTED]

[REDACTED]

Jayakumar Deposition, at 167:10–25 (“Q. You referenced an enhanced financial filtering system that was in place as of December 2022. When did that system first become operable? A. I believe around Q4 of 2021. Q. Prior to Q4 of 2021, was there any filtering of financial data? [...] THE WITNESS. Yes, there was filtering of potentially sensitive financial information prior to 2021. Post-2021, as I defined as the enhanced financial filtering, was applied [REDACTED].”).

103

See, e.g., [REDACTED]

[REDACTED]

104

See, e.g., [REDACTED]

[REDACTED]

2. Core Setup

40. In July 2023, Meta began an initial launch of a feature referred to as “Core Setup.”¹⁰⁵,

¹⁰⁶ Core Setup is designed to prevent the transmission of certain types of event data altogether before it can be sent via the Meta Pixel, and detect and filter it out as soon as possible after it reaches Meta’s servers when sent via Conversions API. For the Meta Pixel, Core Setup limits data transmission “client-side” before developers send data to Meta. Because CAPI operates as server-to-server transmissions, the restrictions on custom parameters and URL parameters are applied as soon as possible once CAPI data reaches Meta’s servers.¹⁰⁷

¹⁰⁵ PIXEL_TAX000052702–704 at 702 (“We are rolling out Core Setup, a version of Business Tools that restricts most freeform data to Meta, to the majority of Health and Finance advertisers.”); PIXEL_TAX000052651–681 at 651 (“Beginning July 20, 2023, we are introducing core setup, which includes new capabilities to restrict certain types of data for Meta Business Tools. Core setup helps businesses by helping reduce the potential for information prohibited by our Business Tools Terms from being shared. As part of this launch, Meta Business Tools may restrict data such as custom parameters and certain parts of URLs from being shared through the Meta Pixel, Facebook App Events SDK and Conversions API or Offline Event Sets. Currently, these changes may primarily affect advertisers globally in health and finance verticals, in particular, potential healthcare or financial service providers.”), at 652 (“[Beginning July 20 to July 26] Some advertisers within health and finance verticals, in particular, potential healthcare or financial service providers, will start receiving in-product notifications in Events Manager and Ads Manager about these changes as applicable. Advertisers will also be notified via email if the core setup feature has been enabled for them.”).

Core Setup was previously called [REDACTED]


¹⁰⁶ Meta implemented at least some of the code related to the functionality of Core Setup in June 2023. *See*

¹⁰⁷ [REDACTED] . *See also* PIXEL_TAX000058628–649 at 637 [REDACTED]

41. Core Setup’s data restrictions are turned on if the Meta Business Tool is associated with domains Meta classifies as finance-related (*i.e.*, “classification-based” enrollment).¹⁰⁸ A developer cannot choose to remove its Pixel ID from Core Setup once it has been placed into Core Setup by Meta.¹⁰⁹

42. As demonstrated by my analysis below, the Meta Pixel IDs operating on both the H&R Block and TaxAct websites are currently enrolled in Core Setup. If the Meta Pixel configured on a website is placed into Core Setup, the specific code responsible for that Meta Pixel’s

Jayakumar Deposition, at 180:7–13



¹⁰⁸ Jayakumar Deposition, at 181:10–23 (“Q. And is Core Setup mainly directed to health and finance advertisers? A. Core Setup is [...] can be applied or is applied to larger categories of -- larger amount of sensitive categories beyond health and finance, and is also a setting that advertisers can opt their Pixel into. Q. Is Core Setup mandatory for health and finance websites? [...] THE WITNESS. Event Data from domains that Meta has categorized as being related to health and finance are placed into Core Setup by Meta.”). *See also*, PIXEL_TAX000058628–649 at 637 (“A Business Tool may be enrolled in core setup for reasons including: Classification-based enrollment: Association with domains or apps classified as health or financial-restricted [...] [or] Escalation-based enrollment: Repeatedly sending parameters that meet the [Signals Integrity System] potentially sensitive data detection thresholds to be designated for [REDACTED]”).

¹⁰⁹ “About Core Setup,” *Meta Business Help Center*, <https://www.facebook.com/business/help/124742407297678>, accessed October 16, 2025 (“If you (or someone on your account) selects a category that comes with restrictions, Meta’s core setup may be applied to your datasets by default. Removing those categories that come with restrictions may also turn off core setup for these Business Tools – unless you have specifically opted in to a core setup or if Meta has placed your pixel in a core setup (for example if the majority of events come from a data source category that comes with restrictions).”); “How to Turn Data Restrictions On and Off in Meta Events Manager,” *Meta Business Help Center*, <https://www.facebook.com/business/help/423150200627651>, accessed October 16, 2025 (“If Meta has turned on data restrictions for your Meta Business Tool, you won’t be able to turn data restrictions off.”).

functionality will load the [REDACTED] plugin.¹¹⁰ I reviewed the *hrblock.com* and *taxact.com* sites and found that both sites contained Meta Pixel code that loads the “ProtectedDataMode” plugin, as shown in **Figure 5** and **Figure 6**.

Figure 5: The [REDACTED] Plugin Is Loaded by the Meta Pixel Code Equipped on *hrblock.com*¹¹¹

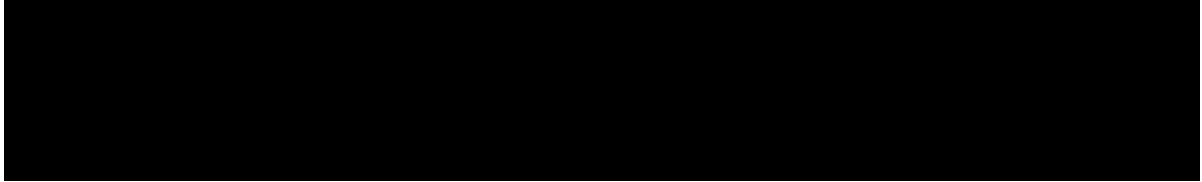
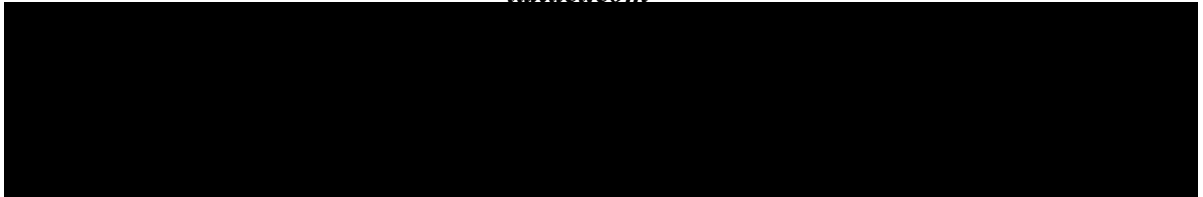


Figure 6: The [REDACTED] Plugin Is Loaded by the Meta Pixel Code Equipped on *taxact.com*¹¹²



43. Consistent with Core Setup functionality, URLs included in the data developers sent to Meta via the Meta Pixel are truncated (see **Figure 7** and **Figure 8**) on both H&R Block and TaxAct websites.¹¹³

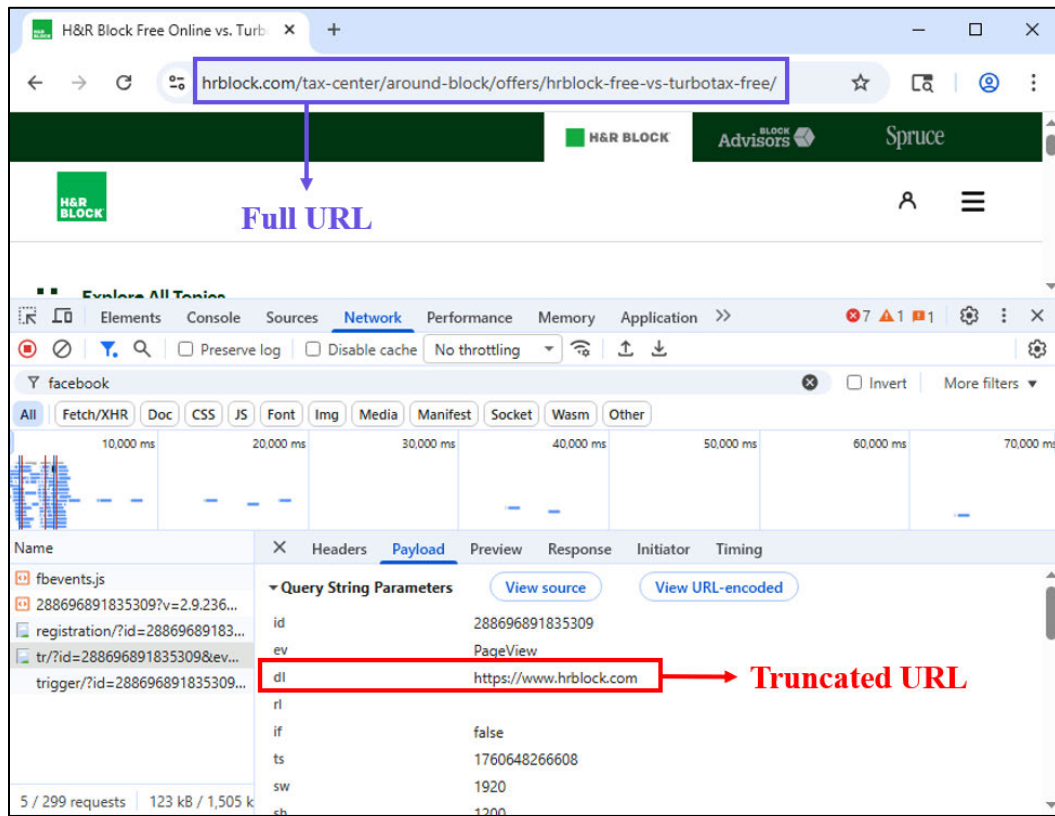
¹¹⁰ This is reflected in the JavaScript file retrieved by the GET request to <https://connect.facebook.net/signals/config/>. See [REDACTED]

and backup materials.

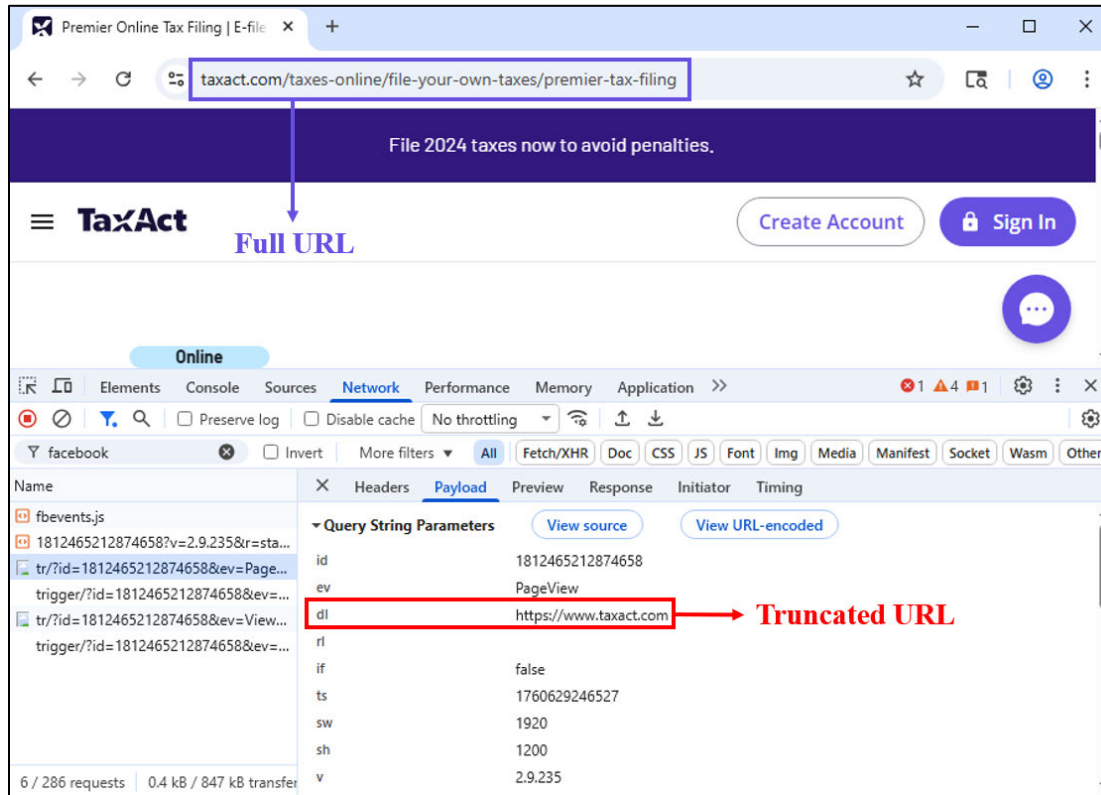
¹¹¹ See **Appendix D**; “windows_chrome_hrblock_default,” which contains the relevant JavaScript file as text (“288696891835309.txt”), in my produced backup materials.

¹¹² See **Appendix D**; “windows_chrome_taxact_default,” which contains the relevant JavaScript file as text (“1812465212874658.txt”), in my produced backup materials.

¹¹³ See PIXEL_TAX000058628–649 at 637 (“Core setup is a Meta Business Tools configuration that, when applied to a particular Business Tool (e.g. a Meta Pixel), restricts certain data like custom parameters and full URLs. When Meta receives an event from a Business Tool in core setup that contains custom parameters and/or a full URL, custom parameters will be discarded and URL will be truncated to just the domain (‘server-side’ core setup functionality).”).

Figure 7: Full URLs Are Not Transmitted Alongside *dl* Parameter on hrblock.com¹¹⁴

¹¹⁴ The URL parameter *dl* contains the URL of the page being visited, and the URL parameter *rl* contains the URL of the previous page visited by the user. See **Appendix D**; “windows_chrome_hrblock_subpage.har” in my produced backup materials.

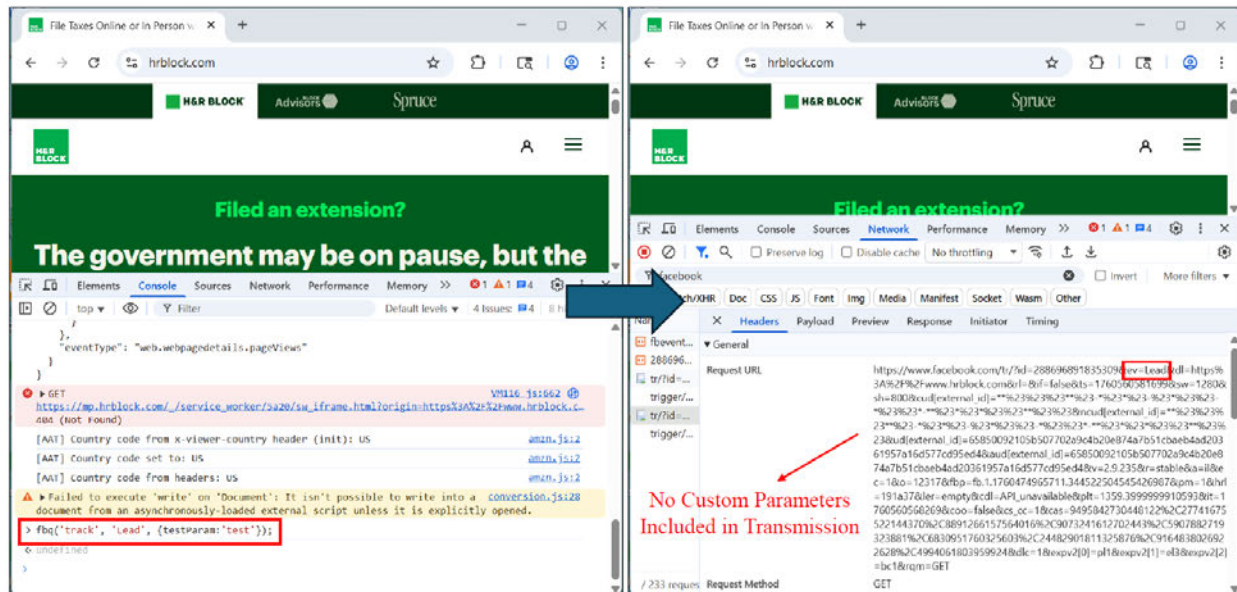
Figure 8: Full URLs Are Not Transmitted as *dl* Parameter on taxact.com¹¹⁵

44. As confirmed by my testing (see **Figure 9**), a website associated with a Pixel ID in Core Setup cannot transmit custom parameters via the Meta Pixel.¹¹⁶

¹¹⁵ The URL parameter *dl* contains the URL of the page being visited, and the URL parameter *rl* contains the URL of the previous page visited by the user. See **Appendix D** and “windows_chrome_taxact_subpage.har” in my produced backup materials.

¹¹⁶ PIXEL_TAX000058628–649 at 637 (“Core setup is a Meta Business Tools configuration that, when applied to a particular Business Tool (e.g. a Meta Pixel), restricts certain data like custom parameters and full URLs. When Meta receives an event from a Business Tool in core setup that contains custom parameters and/or a full URL, custom parameters will be discarded and URL will be truncated to just the domain (‘server-side’ core setup functionality).”).

Figure 9: A Pixel ID Placed into Core Setup Cannot Send Custom Parameters in Event Data Transmissions¹¹⁷



3. *Notifications*

45. Meta has developed a system of notifications to alert developers when potentially sensitive data transmissions are detected or filtered, including sending notifications to developers via email and in Events Manager.¹¹⁸ These notifications alert the developer that Meta has identified

117 As a part of my testing, I use the Chrome browser’s console to run JavaScript code, meant to generate a Standard Event with custom parameters, based on an action taken on the *hrblock.com* site. I observe that while the event data transmission occurs, custom parameters are dropped. The URL parameter *dl* contains the URL of the page being visited, and the URL parameter *rl* contains the URL of the previous page visited by the user. See **Appendix D** and “windows chrome hrblock customParameter.har” in my produced backup materials.

118 Jayakumar Deposition, at 192:8–193:4 (“Q. And you used the word ‘alerts,’ what were you referring to there? [...] THE WITNESS. [...] as I described earlier generally, for systems and products there are mechanisms for the -- to help the teams that maintain these systems to be alerted when certain values or metrics aren’t operating the way they would expect and have the ability to set up monitoring of the health of a system, for example. Alerts refers to the maintenance of a product or system, and is a functionality that can be leveraged by a team. Q. Are alerts distinct or different from notifications that may go out to a website developer saying, Hey, we’ve detected potentially sensitive information? [...] THE WITNESS. It can include what you have described as well, yes”); PIXEL_TAX000058628–649 at 643 (“Meta has processes for notifying third-party developers about enforcement actions taken by SIS when PSD is filtered or data from a prohibited source is discarded. Notifications may be provided in Meta’s Events Manager surface, with detailed diagnostic information, resources, and instructions to evaluate and, if necessary, fix their integration to avoid sending data Meta does not allow. Notifications may additionally be provided via email with links to Events Manager.”); Jayakumar Deposition, Exhibit 141, ¶ 9 (“When Meta’s systems detect and filter our data they categorize as potentially sensitive, Meta sends notifications to the developer (1) via email and (2) in two locations in Meta’s developer


and blocked certain data that may not be in compliance with Meta’s terms.¹¹⁹ The notifications also provide specific information about the affected data, such as the URL where the data was removed, the location of the potentially non-compliant data (but not the content because it is blocked), recommended steps to resolve the issue, and a contact email for further questions.¹²⁰

IV. PLAINTIFFS’ EXPERTS’ PROPOSED METHODOLOGIES FOR COUNTING VISITS TO THE H&R BLOCK AND TAXACT WEBSITES ARE FLAWED

46. Mr. Zeidman claimed that he can determine the number of visits (*i.e.*, the “Visitation Count”¹²¹) to the H&R Block and TaxAct websites using only data from certain fields in the

dashboard, Events Manager. These notifications inform the developer that Meta detected and blocked data that may not comply with Meta’s terms; confirm that the removal may affect ad performance; and provide details about the affected data, including the URL where the events occurred, the locations (but not the contents) of the potentially violating information, steps the developer can take to address the issue, and an email address to contact with questions.”).

See, e.g.,



¹¹⁹ Jayakumar Deposition, Exhibit 141, ¶ 9 (“These notifications inform the developer that Meta detected and blocked data that may not comply with Meta’s terms[.]”).

¹²⁰ Jayakumar Deposition, Exhibit 141, ¶ 9 (“These notifications [...] confirm that the removal may affect ad performance; and provide details about the affected data, including the URL where the events occurred, the location (but not the contents) of the potentially violating information, steps the developer can take to address the issue, and an email address to contact with questions.”).

¹²¹ According to Mr. Zeidman, “a reasonable measure of a ‘visit’ to a website (including the Tax Preparers’ websites) would be each time someone (a) goes to the website and either simply remains for a time on the initial web page or performs some operations such as entering information into the website, and then (b) leaves the website by navigating to a different website, closing the browsing session or timing out. If this visitor comes back to the website again at a later time, that would be considered a second visit. I call the count of these visits a ‘Visitation Count.’” Zeidman Report, ¶ 51.

██████████ table Meta produced,¹²² including: (1) ██████████ limited to the identifiers for the H&R Block or TaxAct website;¹²³ (2) ██████████
 ██████████^{125,126} and (3) ██████████.¹²⁷ Mr. Zeidman claimed that, when filtered as described above, the count of ██████████ is an accurate count of visits to the H&R Block and TaxAct websites.^{128, 129}

47. Mr. Weir’s proposed methodology “to determine the counts of records contained in Meta’s databases”¹³⁰ focused on the same fields in the ██████████ table, including: (1) ██████████ limited to the identifiers for the H&R Block or TaxAct website; (2)

¹²² Zeidman Report, ¶ 53 (“In the below Table 1, I identify the definitions that Meta provided for relevant fields in the Event Data Sample from the ██████████ database. *See* Exhibit P (PIXEL_TAX000034479-506) at 1-2. I am relying on these definitions and also my observations of the data in the fields.”).

¹²³ According to Mr. Zeidman’s analysis, the H&R Block Pixel ID is 288696891835309 and the TaxAct Pixel ID is 1445099202415763. Zeidman Report, ¶ 54.

¹²⁴ Zeidman Report, ¶ 17 (“A ‘browser’ is a computer program used for displaying text, images, and sound over the Internet or an intranet.”).

¹²⁵ Zeidman Report, ¶ 18 (“A ‘server’ is a computer on a network (such as an intranet or the Internet) that is dedicated to a particular purpose, stores information, and serves that information to one or more client computers over the network.”).

¹²⁶ Zeidman Report, ¶ 55 (“Next, the ██████████ should be limited to only ██████████. *See* Exhibit P at 1. *See also*, Exhibit Q (PIXEL_TAX000059048-53) at 3.”).

¹²⁷ Zeidman Report, ¶ 56 (“Finally, the ██████████ Exhibit P at 2.
 ██████████
 ██████████

¹²⁸ Zeidman Report, ¶ 56.

¹²⁹ Mr. Zeidman based his calculation of website visits solely on data from Meta’s ██████████ table (Zeidman Report, ¶¶ 51–53), citing Meta’s description of it as the “source of truth for event data analysis” (Zeidman Report, ¶ 25). However, an accurate count of total visits to H&R Block and TaxAct websites cannot only rely on the data in the ██████████ table because that table may not accurately capture visits to the H&R Block and TaxAct websites—only those that transmitted data to Meta. Certain visits may not generate data transmissions to Meta, such as visits from users using certain browsers (*e.g.*, Safari and Firefox) in private mode or employ ad-blocking tools, preventing data transmissions to Meta (as discussed in **Section VII.A.1**). As a result, Meta’s data from Meta’s ██████████ table does not and cannot reflect the total number of site visits during the proposed class periods.

¹³⁰ Weir Report, ¶ 3 (“I have been asked whether it would be possible to process data obtained from Defendant Meta. Specifically, I have been asked to determine whether it would be possible to determine the counts of records contained in Meta’s databases that meet certain criteria[.]”).

and (3)

.¹³¹

A. The Proposed Methodologies for Counting Visits to the H&R Block and TaxAct Websites Are Unreliable

1. Mr. Zeidman’s Assumption that Each Equates to a Unique Website Visit is Unsupported

48. Mr. Zeidman’s assumption that count equals the count of website visits is unsupported. This assumption would only work if Meta’s definition of a website session was identical to Mr. Zeidman’s definition of a website visit. However, I have not found any support for that. Mr. Zeidman’s definition of a website visit is imprecise and subject to variations in interpretation, and he offers no explanation or support for how Meta defines a website session, much less a way to reconcile any such definition with his imprecise definition of a website visit.

49. Mr. Zeidman defined a website visit as “each time someone (a) goes to the website and either simply remains for a time on the initial web page or performs some operations such as entering information into the website, and then (b) leaves the website by navigating to a different website, closing the browsing session or timing out.”¹³²

50. From a technical perspective, there is no universally accepted definition for a website visit. The definition of a website visit can vary depending on how the start and end of a visit is defined, such as whether the end of a visit occurs after a period of inactivity on the website or after the user leaves the website (or either of the two).¹³³ The period of time that marks the end

¹³¹ Weir Report, ¶¶ 6, 9, 11.

¹³² Zeidman Report, ¶ 51.

¹³³ Huntington, Paul, et al., “Website Usage Metrics: A Re-assessment of Session Data,” *Information Processing & Management*, 44(1), 2008, 358–372, p. 359 (“Unfortunately, despite the undoubted value of this metric in identifying online activity and denoting information seeking behaviour, there are real problems associated with identifying sessions in the logs because there is no way of telling from the transactional log file that a user’s session has come to an end. Hardly anyone logs off from a site, they simply leave the site and this is conducted quite anonymously as far as the logs are concerned.”).

of a website visit can also vary. For example, it can be after a certain number of minutes of user inactivity on the website or at the end of the day.¹³⁴

51. Mr. Zeidman did not define what his phrase “remains for a time” on the initial webpage means (*e.g.*, whether a few seconds or several minutes), nor did he explain whether this time duration should differ by subdomain (*e.g.*, homepage or tax filing page). Moreover, Mr. Zeidman [REDACTED]

[REDACTED]¹³⁵ Mr. Zeidman’s testimony suggests that, if a user stops interacting with a website but leaves a tab to the website open, and then resumes interacting with the website sometime later, his proposed methodology could count such an instance as [REDACTED] even though the user navigated to the website once. In short, Mr. Zeidman’s definition of a website visit is imprecise and sensitive to variations in interpretation and therefore cannot serve as a consistent or reliable definition for purposes of counting visits to the Tax Preparers’ websites.

52. Moreover, Mr. Zeidman did not provide any evidence that Meta defines [REDACTED] the same way he defines a website visit. Thus, Mr. Zeidman’s assumption that [REDACTED] count equals the count of website visits is unsupported.

¹³⁴ Meiss, Mark, et al., “What’s in a Session: Tracking Individual Behavior on the Web,” *HT ’09: Proceedings of the 20th ACM Conference on Hypertext and Hypermedia*, June 29, 2009, p. 178 (“The straightforward approach of identifying sessions using inactivity timeouts thus seemed promising, so we experimented with a variety of different timeouts to find an optimal value. [...] All the statistics we examined (mean number of sessions per user, session duration, number of requests, and number of hosts contacted) turn out to exhibit strong and regular dependence on the particular timeout used.”).

¹³⁵ Deposition of Robert Zeidman, (“Zeidman Deposition”), October 3, 2025, at 180:23–181:3 (“Q. And it’s [REDACTED], right? A. My wife, too, yes. Q. Drives me insane. A. I know.”).

2. *Methodologies for Counting Visits to the H&R Block and TaxAct Websites Count Visits from Non-Humans*

53. Because Mr. Zeidman’s and Mr. Weir’s methodologies for counting the number of visits to the H&R Block and TaxAct websites rely only on filtering data from certain fields in the [REDACTED] table, the counts of website visits would include visits generated by bots.

54. Bot activity on the internet exists and may be challenging to detect.¹³⁶ For example, one study estimates that 32% of internet traffic comes from bots.¹³⁷ Mr. Zeidman testified that his methodology for counting the number of visits to the H&R Block and TaxAct websites does not filter out website visits from bots, and visitation counts using his methodology include website visits from bots.¹³⁸ Since neither Mr. Zeidman nor Mr. Weir offers any methodology to exclude bot traffic, their methodologies overstate the number of genuine user visits to the H&R Block and TaxAct websites reflected in the [REDACTED] table, because they may include website visits from bot traffic.

B. The Proposed Methodologies for Counting Visits to the H&R Block and TaxAct Websites Cannot Be Used to Exclude Visits from Users Who Provided Consent

55. Counsel for Meta asked me to assess whether Mr. Zeidman’s and Mr. Weir’s proposed methodologies to count the number of visits to the H&R Block and TaxAct websites

¹³⁶ Imperva, “2024 Bad Bot Report, 2024, p. 3 (“Bad bots interact with applications in a way that mimics legitimate users, making them more challenging to detect and block.”).

¹³⁷ “2024 Bad Bot Report,” Imperva, <https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/>, accessed October 27, 2025 (“The 2024 Imperva Threat Research report reveals that almost 50% of internet traffic comes from non-human sources. Bad bots, in particular, now comprise nearly one-third of all traffic. Bad bots have become more advanced and evasive and now mimic human behavior in such a way that it makes them difficult to detect and prevent.”).

¹³⁸ Zeidman Deposition, at 179:14–24 (“Q. A bot could certainly crawl the site, right? A. It could crawl the site, yes. Q. So under the current visitation count, that would include bot visitors, right? A. I think that’s correct. That’s something I would want to look into. There may be a way of identifying bots, but I think that’s a possibility. Q. Your methodology thus far does not attempt to filter out bots in any way, right? A. That’s correct.”).

during the proposed class periods can be used to exclude website visitors who provided consent.¹³⁹ Their proposed methodologies cannot be used to exclude such visits, and I am not aware of a method to reliably do so.

C. Methodologies for Counting Visits to the H&R Block and TaxAct Websites Cannot Be Used to Count Visits from Individuals in California

56. As discussed in **Section I.D**, certain proposed classes include individuals in the United States who visited the H&R Block and TaxAct websites, while other proposed classes are limited to individuals in the State of California who visited those websites. Counsel for Meta asked me to assess whether Mr. Zeidman’s and Mr. Weir’s proposed methodologies to count the number of visits to the H&R Block and TaxAct websites during the proposed class periods can be used to identify the locations of website visitors when they accessed the H&R Block or TaxAct websites. For the reasons discussed below, their methodologies cannot be used to identify the locations of website visitors when they accessed the websites.

57. Mr. Weir did not offer a method to determine the location of website visitors. Mr. Zeidman noted that data transmitted to Meta via the Meta Pixel included fields such as [REDACTED] [REDACTED]”¹⁴⁰ Meta’s data dictionary indicates the fields [REDACTED]

¹³⁹ I discuss the presence of consent banners on the H&R Block and TaxAct websites during the class period in **Appendix D; Section III.C**.

¹⁴⁰ Zeidman Report, ¶ 29 [REDACTED]

[REDACTED] Exhibit H (PIXEL TAX000058898–905) at 1–2.”); Exhibit H [REDACTED]

58. As an initial matter, ZIP codes inferred from IP addresses can be imprecise proxies for website visitors' true geolocations,¹⁴³ and may therefore not necessarily reflect a user's actual location when visiting the H&R Block and TaxAct websites. This would likely lead to some visits to the H&R Block and TaxAct websites being identified as coming from individuals inside or outside of the State of California instead of users' actual location when visiting the H&R Block and TaxAct websites.¹⁴⁴

¹⁴¹ PIXEL TAX000058898–905 at 899–900

¹⁴² Zeidman Deposition, at 150:16–20 (“Q. So in any event, IP addresses may not be a particularly precise method for evaluating a physical location for the reasons we’ve discussed, right? A. That’s correct.”).

¹⁴³ Donnini, Fernanda, “How Accurate Is IP Address Location? Geolocation Information & More,” *IPinfo*, <https://ipinfo.io/blog/ip-address-location-accuracy>, accessed October 20, 2025 (“Like a physical address, an IP address points to a specific location in the online world. These IP addresses are documented in public WHOIS records [...] When an internet device connects to a website via an ISP [Internet Service Provider], it shares its IP address with that site. Depending on the IP address data provider that site is using, geolocation is determined by the WHOIS information, along with routing information and other relevant data. This process, however, is imperfect, given that WHOIS location data is unregulated and provided voluntarily by ASNs [Autonomous System Number].”).

¹⁴⁴ Nur, Abdullah Yasir, “Accuracy and Coverage Analysis of IP Geolocation Databases,” *International Balkan Conference on Communications and Networking (BalkanCom)*, 2023, pp. 1–6 (“In this paper, we evaluate the coverage and accuracy of four widely used IP geolocation databases[.] [...] We use the ground truth dataset to evaluate the accuracy of the databases. Our results show that the four databases’ average distance discrepancy mean is 376 km.”).

59. This dynamic is compounded by tools that mask IP addresses. VPNs¹⁴⁵ (e.g., NordVPN, Surfshark, or IPVanish)¹⁴⁶ and proxy servers¹⁴⁷ (e.g., Apple’s Private Relay¹⁴⁸) replace a user’s public IP address with one provided by the service, which may resolve to another state or

¹⁴⁵ A VPN can mask the public IP address of the user’s router with the VPN’s IP address. While VPNs were typically offered for desktop users, their usage on mobile devices has increased. *See, e.g.,* Corrons, Luis, “What Is a VPN and What Does It Do?” *Norton*, April 9, 2024, <https://us.norton.com/blog/privacy/what-is-a-vpn>, accessed October 9, 2025 (“VPN stands for virtual private network—it’s technology that encrypts your data when you use the internet, scrambling it so that strangers on the same network can’t read it. A VPN creates a secure tunnel between your device and the internet to protect data during transmission. This secure tunnel helps VPNs disguise your IP address, mask your online activity (including links you click and files you download), and hide your physical location to help you access your favorite content.”); Buxton, Oliver, “What Does a VPN Hide? 6 Common Identifiers VPNs Disguise,” *Norton*, February 21, 2025, <https://us.norton.com/blog/privacy/what-does-a-vpn-hide>, accessed September 22, 2025 (“[A] VPN can make some of your digital footprints virtually untraceable by hiding your IP address, location, browsing history, and even the files you download[.]”); “What Is a VPN?,” *Microsoft Azure*, <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn>, accessed October 20, 2025 (“While long-standing VPN providers typically cater toward desktop users, smartphones have spurred a huge uptick in growth among VPNs for mobile—and for good reason. For smartphone users looking for greater security and protection while on the go, a mobile VPN is a necessity.”).

¹⁴⁶ “Dedicated NordVPN IP Addresses,” *NordVPN Support Center*, <https://support.nordvpn.com/hc/en-us/articles/19507808024209-Dedicated-NordVPN-IP-addresses>, accessed October 20, 2025 (“When using NordVPN, your IP address changes to that of your VPN server. Normally, you share this IP address with other NordVPN users connected to the same server.”); “Hide My IP: Stay Private Online with Surfshark VPN,” *Surfshark*, <https://surfshark.com/features/hide-ip>, accessed October 27, 2025 (“When you equip a VPN, your chosen VPN server’s IP will mask your actual address. Any website you visit won’t see who you are unless you do something to reveal yourself.”); “What Is a VPN?,” *IPVanish*, <https://www.ipvanish.com/what-is-a-vpn/>, accessed October 12, 2025 (“When your VPN connection is active, your IP address will match your VPN server’s IP addresses. To the rest of the internet, such as the website you visit, you’ll appear as if you’re actually connecting from your server’s location rather than your true physical location.”).

¹⁴⁷ Proxy servers work similarly to VPNs, providing IP addresses that mask the public IP addresses of users’ gateway devices. *See, e.g.,* Dutta, Nitul, Nilesh Jadav and Sudeep Tanwar, *Cyber Security: Issues and Current Trends*, Studies in Computational Intelligence, 2022, p. 60 (“In another scenario, if the employee uses a proxy server, the proxy will change the source IP address to some random address. [...A VPN] works similar to a proxy but with a minute difference, such as proxy act as a man-in-the-middle server for an application such as torrent client or web browser. In contrast, VPN captures all the traffic from every application which is running on the computer and tunnels it through an encryption mechanism to tackle privacy concerns”).

¹⁴⁸ *See, e.g.,* Hodge, Rae, “No, Apple’s Private Relay Is Not a VPN, but You Can Still Try It Out with iOS 15,” *CNET*, February 10, 2022, <https://www.cnet.com/tech/services-and-software/no-apples-private-relay-is-not-a-vpn-but-you-can-still-try-it-out-with-ios-15/>, accessed September 15, 2025.

even another country.¹⁴⁹ In 2019, at least a quarter of Americans used a VPN or proxy server to access the Internet,¹⁵⁰ and by 2023, VPN usage alone increased to a third of Americans.¹⁵¹

60. To illustrate how VPNs operate, I used the *whatismyip.com* service that displays the IP address detected for the user visiting the website. As shown in **Figure 10** below, when visiting the website without VPN, my IP address was identified to be 13.91.95.204¹⁵² and my location in California. However, when I enabled my VPN application, as displayed in **Figure 11**, the detected IP address changed to 193.160.100.137 and was inferred to be located in Finland. Mr. Zeidman affirmed in his deposition testimony that a website visitor in California using a VPN might appear to be in “Europe somewhere.”¹⁵³

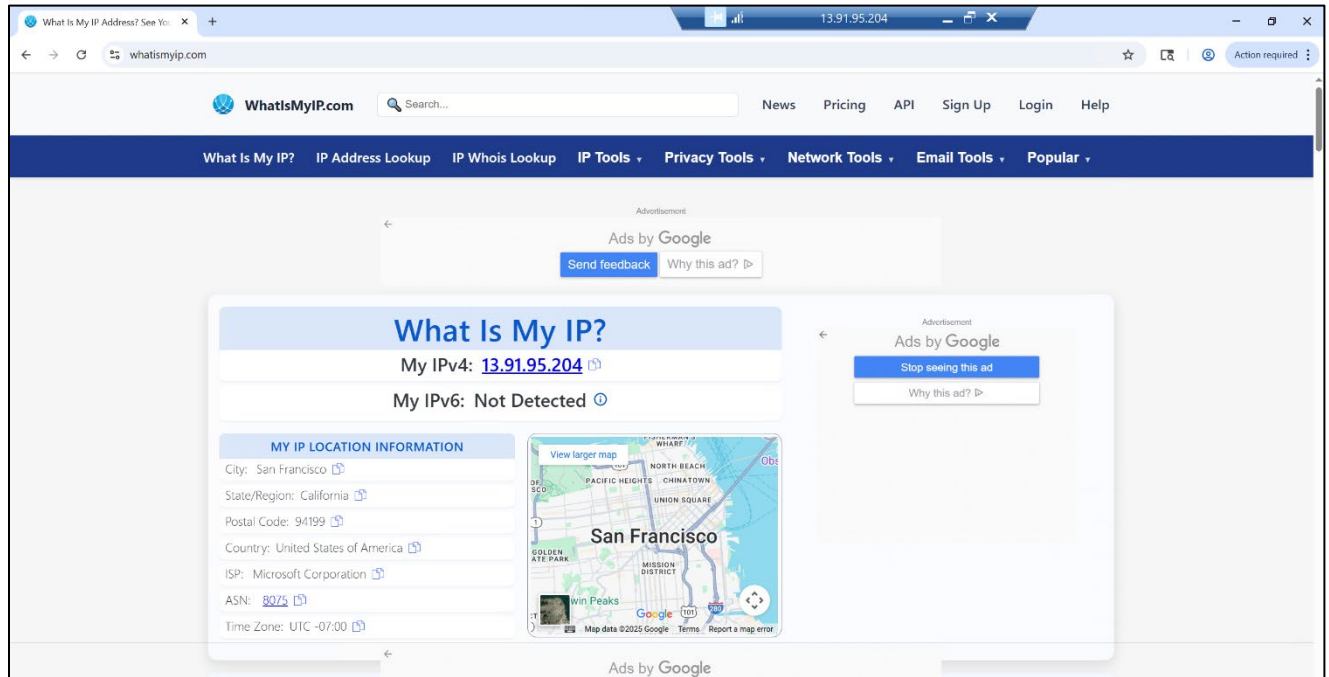
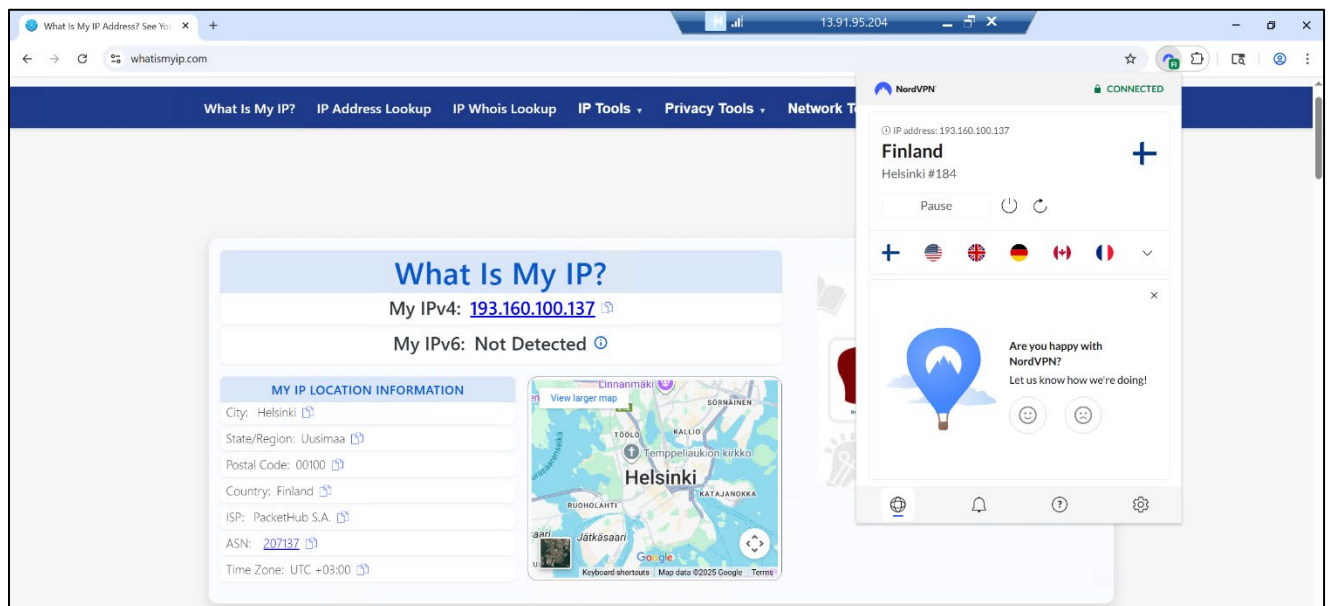
¹⁴⁹ Day, Brett, “What a VPN Hides (And What It Doesn’t),” *Forbes*, September 26, 2025, <https://www.forbes.com/advisor/business/software/what-does-vpn-hide/>, accessed October 20, 2025 (“[A] VPN masks the IP address that is assigned to you by your internet service provider (ISP), meaning you can be anonymous while online. With a VPN, you can trick snoopers, [...] into thinking you’re located in another city or country. [...] With a VPN, your IP address is masked and replaced with an IP address assigned by the VPN.”); Hoory, Leeron, “What Is a Proxy Server?” *Forbes*, September 10, 2025, <https://www.forbes.com/advisor/business/what-is-a-proxy-server/>, accessed October 20, 2025 (“People use proxy servers to assume a geographic location, whether they are [physically] there or not,” Chris Mattmann, chief data and AI officer at UCLA, explains.”).

¹⁵⁰ 25% of American Internet users used a VPN or proxy server in just the month prior to GlobalWebIndex’s Q4 2019 survey of Internet users aged 16 to 64. See Top10VPN.com and GlobalWebIndex.com, “Global VPN Usage Report 2020,” 2020, p. 5.

¹⁵¹ Globyte, Ema, “NordVPN Survey Shows: A Third of Americans Use a VPN,” *NordVPN*, June 28, 2023, <https://nordvpn.com/blog/nordvpn-usage-survey-us/#header-end>, accessed September 15, 2025 (“The survey shows that VPN awareness and usage are above average in the U.S., making it one of the leading countries out of the 18 participating in the study. Two in three people (66.8%) in the U.S. know what a VPN is, with a third of Americans (33.0%) saying they use it. VPN usage has increased considerably since 2022, from just under a quarter (24.3%) to a third”).

¹⁵² I conducted this test using a California-based virtual machine. See **Appendix D**.

¹⁵³ Zeidman Deposition, at 131:16–19 (“Q. So, for example, if I use a VPN from California, I might show up as being in Europe somewhere? A. That’s correct.”).

Figure 10: Site Visit Reflects Approximate Actual Location of Device Before VPN Is Enabled¹⁵⁴**Figure 11: Site Visit Reflects VPN-Assigned Location After VPN Is Enabled¹⁵⁵**¹⁵⁴ See Appendix D.¹⁵⁵ See Appendix D.

61. Thus, VPNs and other tools that mask IP addresses are another reason why data inferred from geo IP location are unreliable to count the number of visits made to the TaxAct and H&R Block websites by individuals in California, and Mr. Zeidman’s methodology does not propose any other approach. Mr. Zeidman’s reliance on imprecise¹⁵⁶ and unreliable¹⁵⁷ proxies for website visitors’ true geolocations means that his proposed methodology is not a reliable way to identify the locations of website visitors and count the number of visits made to the H&R Block and TaxAct websites in California.

V. PLAINTIFFS’ EXPERTS’ PROPOSED METHODOLOGIES TO COUNT WEBSITE VISITS ARE INCAPABLE OF ACCURATELY IDENTIFYING VISITORS TO THE H&R BLOCK AND TAXACT WEBSITES

62. Counsel for Meta asked me to assess whether Mr. Zeidman’s and Mr. Weir’s proposed methodologies to count the number of visits to the H&R Block and TaxAct websites during the proposed class periods can be used to accurately identify visitors to the H&R Block and TaxAct websites during the proposed class periods. I found that their methodologies are incapable of doing so.

63. Mr. Zeidman noted in his report that he reviewed the number of [REDACTED] and associated ZIP codes in the [REDACTED] table and determined based on that information that there are “numerous people” who visited the H&R Block and TaxAct websites during the proposed class periods.¹⁵⁸ But [REDACTED] cannot always be used to track a specific

¹⁵⁶ Zeidman Deposition, at 150:16–20 (“Q. So in any event, IP addresses may not be a particularly precise method for evaluating a physical location for the reasons we’ve discussed, right? A. That’s correct.”).

¹⁵⁷ Zeidman Deposition, at 131:16–19 (“Q. So, for example, if I use a VPN from California, I might show up as being in Europe somewhere? A. That’s correct.”).

¹⁵⁸ Zeidman Report, ¶ 43 (“I have reviewed the Event Data Sample, particularly from the [REDACTED] spreadsheet. By reviewing the number of unique (encrypted) IP addresses and associated zip codes, I have determined that there are numerous (and more than 40) people who visited the HRB and TaxAct websites, both nationally and in California, during the relevant class periods.”).

user or device for several reasons: (1) public IP addresses can be shared across multiple devices and users on the same network, and users may connect to multiple public IP addresses even within a short period of time; (2) IP addresses change over time, meaning that a single user may have multiple IP addresses during the proposed class periods; and (3) VPNs and proxy servers allow users to change their IP addresses. Thus, IP addresses are insufficient for accurately identifying visitors to the H&R Block and TaxAct websites.

64. First, public IP addresses are assigned by Internet Service Providers (“ISPs”) to computers or routers, in which case all devices on the same local network share the same public IP address.¹⁵⁹ For example, a library with a single router accessing the internet can have one ISP-assigned internet-facing IP address. That router will then assign internal IP addresses to all devices within the library network so that internal traffic can be routed. Therefore, the librarian using the TaxAct website during a break and the public library user accessing the TaxAct website on a public computer will appear to computers outside of the library’s network as using the same ISP-assigned IP address. In addition, IP addresses change when users switch networks (*e.g.*, moving between home, work, or public Wi-Fi).¹⁶⁰ To extend the example, imagine that the librarian and the public

¹⁵⁹ Bodnar, Danielle, “Public vs. Private IP Address: Understanding the Differences,” *Norton*, April 24, 2025, <https://us.norton.com/blog/privacy/public-vs-private-ip-address>, accessed October 20, 2025 (“To help protect the privacy of individual network users, multiple devices within a local network often share a single public IP address hosted by the router, utilizing private IP addresses to communicate internally within the local network.”). *See also*, Zeidman Deposition, at 147:19–148:1 (“Q. An individual user can be associated with multiple IP addresses, right? A. That’s correct. Q. For example, their phone may have one -- their browser on their phone may have one, their computer may have another, and some other device may have a third? A. That’s correct.”); “A Better Alternative to IP Whitelisting,” *OpenVPN*, December 18, 2024, <https://blog.openvpn.net/ip-whitelisting>, accessed October 20, 2025 (“The majority of users will have dynamic IP addresses because that is how most internet service providers assign IPs. A lot of dynamic addresses are renumbered every 24 hours or some multiple of 24 hours. Outages can also lead to an IP address change.”).

¹⁶⁰ “Static vs. Dynamic IP Address,” *Fortinet*, <https://www.fortinet.com/resources/cyberglossary/static-vs-dynamic-ip>, accessed October 14, 2025 (“Internet service providers (ISPs) temporarily assign dynamic IP addresses via the Dynamic Host Configuration Protocol (DHCP) server. This means an IP address can change every time a user reboots their router or system, and when the user connects to their ISP service.”). *See also*, “NAT Service,” *University of Cambridge*, August 7, 2025, <https://help.uis.cam.ac.uk/service/network-services/datanetwork/nat>, accessed September 16, 2025 (“[S]ingle global IP address to be used by multiple internal hosts with local IP

user go home and each continues to use the TaxAct website. These additional visits will have different IP addresses than those conducted at the library and would therefore look like they are from two additional users.

65. Second, the IP address associated with a user’s device can change over time. Mr. Zeidman testified in his deposition, “IP addresses can be assigned and reassigned, so one device can be reassigned [to] different IP addresses”¹⁶¹ and that this is “done for a lot of users.”¹⁶²

66. Third, VPNs mask a user’s real IP address by substituting it with one provided by the VPN service, so a single user can have multiple VPN-assigned IPs (see **Section IV.C**), and multiple users can also use the same VPN-assigned IP.¹⁶³ For each of these reasons, IP addresses cannot always be used to associate visits with a specific user device and are insufficient for accurately identifying visitors to the H&R Block and TaxAct websites.

67. Further, Mr. Zeidman’s and Mr. Weir’s methodologies rely on the [REDACTED] table, which contains multiple fields potentially relevant to user matching. However, their methodologies do not account for the possibility that, based on the values in these fields, events might not be able to be matched to individual users. For example, my review of the produced schema reveals the [REDACTED]

addresses.”). *See also*, “Maintain Networks with Dynamic IP Addresses,” *Cisco*, September 3, 2025, <https://www.cisco.com/c/en/us/support/docs/security/umbrella/224730-maintain-networks-with-dynamic-ip.html>, accessed September 16, 2025 (“Dynamic IP address means that the public IP of your network changes over time when the lease for that IP address changes.”).

¹⁶¹ Zeidman Deposition, at 147:3–6 (“Q. IP addresses change over time, don’t they? A. Well, IP addresses can be assigned and reassigned, so one device can be reassigned different IP addresses.”).

¹⁶² Zeidman Deposition, at 147:7–12 (“Q. And that’s pretty common? A. I would say it’s done for a lot of users. Many devices have fixed IP addresses, but don’t change, but particularly users that -- individual users, individual computers that go through an ISP, their IP address will change from time to time.”).

¹⁶³ “Dedicated IP,” *NordVPN*, <https://nordvpn.com/features/dedicated-ip/>, accessed October 25, 2025 (“Dedicated IP vs. shared IP[:]. In a VPN context, a shared IP address is an IP address that can be assigned to multiple users connected to the same server at the given time. While a dedicated IP address is a unique string provided by a VPN service or a hosting provider that is assigned to your account exclusively.”).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Plaintiffs’ experts’ methodologies do not account for the possibility that data on user interactions with the H&R Block and TaxAct websites may potentially remain unmatched to users or possibly matched to users who did not actually take the action associated with the event data.

68. Moreover, the produced data does not indicate whether events reflect information entered about the website visitor or about another individual. For example, my review of the [REDACTED] table identified 1,500 events associated with links related to filing taxes for a deceased taxpayer.¹⁶⁹ It is not possible to determine from the produced data whether the website visitor was interacting with the website on their own behalf or on behalf of someone else.

¹⁶⁴ PIXEL_TAX000058843.

¹⁶⁵ See, e.g., PIXEL_TAX000036169–PIXEL_TAX000036268.

¹⁶⁶ See PIXEL_TAX000058843.

¹⁶⁷ See [REDACTED] in my produced backup materials.

¹⁶⁸ See [REDACTED] in my produced backup materials.

¹⁶⁹ I filtered the “[REDACTED]” variable in the [REDACTED] table for values containing the paths [REDACTED]. All matching links are associated with either the *www.hrblock.com* or *www-hrblock-com.cdn.ampproject.org* domains. See “deceased_urls” in my produced backup materials.

VI. MR. ZEIDMAN’S OPINION THAT HE FOUND AN “ENORMOUS AMOUNT OF TAX INFORMATION” AND OTHER DATA TRANSMITTED TO META IS UNRELIABLE

69. Mr. Zeidman opined that he “found [...] an enormous amount of tax information and other data transmitted to Meta from the Tax Preparers’ websites.”¹⁷⁰ However, this opinion is unreliable for the reasons set forth below.

70. In opining that there was purportedly an “enormous amount of tax information and other data transmitted to Meta from the Tax Preparers’ websites,”¹⁷¹ Mr. Zeidman referenced certain parameter names he described as “conform[ing] to tax information.”^{172,173} However, Mr. Zeidman did not reliably assess the prevalence of “tax information” in the data transmissions because: (1) he did not define what he considers “tax information” to be or provide a methodology for doing so; (2) he did not specify what he considers an “enormous amount” or provide a methodology for making such a determination; (3) he included only one example of “tax information” sent by the H&R Block website and ignored H&R Block custom parameters; and (4) my own review demonstrates that the parameters he described as “conform[ing] to tax information”¹⁷⁴ are a small percentage of the data that was sent to Meta.

¹⁷⁰ Zeidman Report, ¶ 57(2).

¹⁷¹ Zeidman Report, ¶ 57(2).

¹⁷² Zeidman Deposition, at 69:14–19 (“THE WITNESS: Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information. I don’t recall the specific details of Exhibit M and Exhibit N, but I could go over them.”).

¹⁷³ Zeidman Report, ¶ 49.

¹⁷⁴ Zeidman Deposition, at 69:14–19 (“THE WITNESS: Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information. I don’t recall the specific details of Exhibit M and Exhibit N, but I could go over them.”).

A. Mr. Zeidman’s Opinions Contain Significant Methodological Flaws

71. Mr. Zeidman failed to define what he considers “tax information” to be or to provide any methodology for making such a determination. Mr. Zeidman testified that he identified certain categories of data as “tax information” because the sample data he reviewed appeared to him to “conform to tax information,” but he did not apply any methodology to test for that.¹⁷⁵ Mr. Zeidman’s failure to take these steps means that he did not reliably assess the prevalence of “tax information” in the data transmissions.

72. However, based on my review of the data produced in this case, Mr. Zeidman ignored that *numChildButtons* appears in the same context as other button properties, such as the button’s text and HTML tag.¹⁷⁶ Moreover, Mr. Zeidman ignored that in web development, “child” is the standard technical term for an element nested inside another “parent” element.¹⁷⁷

73. Mr. Zeidman also ignored that the names of custom parameters are chosen by developers and therefore do not necessarily reflect the content of the information transmitted (see **Section III.A.2**). Developers could, for example, send data that is not tax information in a parameter name that appears to be tax information. Therefore, an attempt to interpret whether events and parameter names constitute tax information, as Mr. Zeidman did, is unreliable.

¹⁷⁵ Zeidman Deposition, at 69:6–20 (“Q. So you reviewed the sample that is pictured on page 14 of your report? A. Yes. Q. And based on that, you determined that the categories listed in paragraph 49 are tax information? THE WITNESS. Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information. I don’t recall the specific details of Exhibit M and Exhibit N, but I could go over them. They were attached to my report.”).

¹⁷⁶ [REDACTED] PIXEL_TAX000023399, row 2821. See also “<button>: The Button element,” *Mozilla Developer Network*, <https://developer.mozilla.org/en-US/docs/Web/HTML/Reference/Elements/button>, accessed October 27, 2025; “HTML <button> Tag,” *W3Schools*, https://www.w3schools.com/tags/tag_button.asp, accessed October 27, 2025.

¹⁷⁷ “Element: Children Property,” *Mozilla Developer Network*, <https://developer.mozilla.org/en-US/docs/Web/API/Element/children>, accessed October 27, 2025.

74. Further, despite purporting to demonstrate “that even the sample provided by Meta shows the Meta Pixel transmitting an enormous amount of tax information,”¹⁷⁸ Mr. Zeidman did not define what he considers an “enormous amount,” nor did he provide a methodology for making such a determination.

75. Instead, Mr. Zeidman noted Meta’s acknowledgement that it received certain data from the TaxAct website¹⁷⁹ and that he further observed that “there are thousands of rows of data like this,” a vague conclusion unsupported by methodology.¹⁸⁰ Mr. Zeidman admitted that he characterized the amount of “tax information” data as “enormous” based solely on the volume of spreadsheets provided by Meta, without verifying the extent to which those spreadsheets actually contained “tax information.”¹⁸¹ Without a clear definition of what “tax information” entails or a methodology for determining what constitutes “tax information,” it is impossible to reliably count or assess the prevalence of such data, let alone describe the amount of such data as “enormous.”

76. Mr. Zeidman’s examples do not support his claim that there was purportedly an “enormous amount of tax information” transmitted to Meta from *both* websites.¹⁸² Mr. Zeidman relied on a single example of “tax information” sent by the H&R Block website—a URL showing

¹⁷⁸ Zeidman Report, ¶ 4(b).

¹⁷⁹ *See, e.g.*, Zeidman Report, ¶¶ 40, 46–47.

¹⁸⁰ Zeidman Report, ¶ 50.

¹⁸¹ Zeidman Deposition, at 71:16–72:9 (“Q. What is your basis for determining that it was an enormous amount of tax information and other data? A. Well, enormous is, of course, a non-technical term, it’s not a quantifiable or quantity; however, the -- the spreadsheets that I received as a sample of data from Meta was, when put into a database, created a database that was as I recall, hundreds of gigabytes over a limited period of time. And it was so much that I had to get a -- one of the top end solid state drives. And as a spreadsheet, it was virtually unusable because the spreadsheet program Excel could not open it -- any one of these, and there were, I believe, hundreds. So Excel had difficulty opening one of them, and putting it into a database took a while to search. So I think although ‘enormous’ is not a technical term, it just meant that there was a very large amount of data by any standard that I’m used to.”), at 73:6–18 (“Q. So you don’t know, as we sit here today, if one percent of the entries or 60 percent of the entries included data of the kind in paragraphs 46, 47, or 49 of your report? A. As I sit here, I don’t recall the exact percentage. Q. You don’t recall or you didn’t calculate it? A. At some point, I looked for the numbers, but I don’t know that I calculated a percentage.”).

¹⁸² Zeidman Report, ¶ 4(b).

that a user visited a webpage discussing the basics of the capital gains tax.¹⁸³ Even assuming it might constitute “tax information,” this is a single data point. Thus, Mr. Zeidman’s example provides virtually no evidence that visitors to the H&R Block website during the proposed class period had “tax information” transmitted to Meta.

77. Indeed, Mr. Zeidman’s opinion regarding the transmission of tax information relies entirely on custom parameters created by TaxAct’s developers to capture and transmit certain data fields through the Meta Pixel.¹⁸⁴ That is, none of the parameters he identified are sent by the H&R Block website. Mr. Zeidman’s opinion that *both* websites sent Meta an “enormous amount of tax information” is unsupported.¹⁸⁵

B. My Independent Review Shows that the Event Data Mr. Zeidman Analyzed Appears Infrequently

78. Mr. Zeidman testified that he did not quantify how often transmission of “tax information” occurred and was not aware if these transmissions represented more or less than 60, 50, 10 or 1 percent of the events.¹⁸⁶ My analysis of the [REDACTED] table for the TaxAct website produced in this matter shows that the parameters Mr. Zeidman referenced¹⁸⁷ appear in only [REDACTED]

¹⁸³ Zeidman Report, ¶ 48.

¹⁸⁴ Zeidman Report, ¶ 49.

¹⁸⁵ Zeidman Report, ¶ 4(b).

¹⁸⁶ Zeidman Deposition, at 71:4–8 [REDACTED]

¹⁸⁷ Zeidman Deposition, at 68:18–69:5 [REDACTED]

of all the events in the samples for the TaxAct website, which corresponds to [REDACTED] [REDACTED] associated with events from the TaxAct website.¹⁸⁸ None of Mr. Zeidman’s purported “tax information” parameters¹⁸⁹ were observed in any of the sample data for the H&R Block website in the [REDACTED] data.¹⁹⁰

79. Further analysis shows that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].¹⁹¹ Excluding events where all parameter values were replaced in the data in the [REDACTED] table that Mr. Zeidman analyzed reduces the share of events Mr. Zeidman described as “conform[ing] to tax information”¹⁹² to [REDACTED] of sampled events from the TaxAct website (corresponding to [REDACTED] associated with events from the TaxAct website).¹⁹³

80. None of the event data produced by Meta for the Named Plaintiffs was associated with TaxAct—not even for Ms. Calderon, the TaxAct classes’ only proposed representative.¹⁹⁴ In addition, Mr. Zeidman did not identify any custom data parameters transmitted by the H&R Block website that he considered to be tax information. I observe that the only custom data parameters in

¹⁸⁸ See “taxact_parameters” in my produced backup materials.

¹⁸⁹ Zeidman Deposition, at 69:6-18 (“Q. So you reviewed the sample that is pictured on page 14 of your report? A. Yes. Q. And based on that, you determined that the categories listed in paragraph 49 are tax information? [...] A. Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information.”).

¹⁹⁰ See “hrblock_parameters” in my produced backup materials.

¹⁹¹ See PIXEL_TAX000036199, row 877.

¹⁹² Zeidman Deposition, at 69:14–19 (“THE WITNESS: Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information. I don’t recall the specific details of Exhibit M and Exhibit N, but I could go over them.”).

¹⁹³ See “taxact_parameters” in my produced backup materials.

¹⁹⁴ The event data associated with the Named Plaintiffs does not contain any observations associated with TaxAct’s Meta Pixel ID. See Zeidman Report, ¶ 49; “named_plaintiff_pixel_ids_and_custom_data” in my produced backup materials.

the Named Plaintiffs’ events data,¹⁹⁵ which only includes events associated with the H&R Block website, are [REDACTED]¹⁹⁶ I reviewed these parameters and determined that none of them are the same as the ten parameters which Mr. Zeidman claims “conform[ed] to tax information.”¹⁹⁷

VII. MR. ZEIDMAN FAILED TO CONSIDER VARIABILITY IN THE DATA DEVELOPERS TRANSMIT VIA THE META PIXEL

81. Mr. Zeidman concluded that “[d]uring the relevant class periods the Meta Pixel operated *in a largely uniform manner* on the Tax Preparers’ websites with respect to the basic mechanics of collecting and transmitting visitor data to Meta.”¹⁹⁸ This conclusion is wrong because Mr. Zeidman ignored important technical details that cause variability in the data transmissions, including the many controls available to users and developers to prevent or limit the transmission of data and the effects of Meta’s technical measures.

82. Below, I describe a variety of circumstances illustrating the types of factors—such as browser settings, user choices, developer configurations, and Meta’s technical measures—that would have led to variation in whether and how data was transmitted, demonstrating that it was not uniform.

¹⁹⁵ See PIXEL_TAX000003583–PIXEL_TAX000003586.

¹⁹⁶ See “named_plaintiff_pixel_ids_and_custom_data” in my produced backup materials.

¹⁹⁷ Zeidman Deposition, at 68:18–69:5 (“Q. [...] So did you do any independent work to determine what each of these categories means? A. Well, I can -- I believe that Meta confirmed, and I have that in Exhibit M in the responses and Exhibit N in responses, and also in paragraph 49 there is an event data sample that provided which has numbers for these fields, which seem to conform with things like [REDACTED]”).

[REDACTED] at 69:6-18 (“Q. So you reviewed the sample that is pictured on page 14 of your report? A. Yes. Q. And based on that, you determined that the categories listed in paragraph 49 are tax information? [...] A. Well, I determined from the information that Meta provided to us, which is given in Exhibit M and Exhibit N, and the event data sample they gave us which all conform to tax information.”).

¹⁹⁸ Zeidman Report, ¶ 40 (emphasis added).

A. Users Have Controls That Prevent or Limit the Transmission of Data via the Meta Pixel

83. Users may prevent the transmission of data via the Meta Pixel in a number of ways which may have varied over time for any given user: (1) using ad blockers or other browser extensions that prevent certain data transmissions; (2) granting or denying consent to certain tracking technologies when presented with consent banners; (3) having or not having previously visited a Meta domain or being logged in to a Meta user account, affecting cookie transmission; (4) using browser-specific controls or using browsers that limit the data developers can send via the Meta Pixel; and (5) choosing to browse in strict or private browsing modes that block developers from sending data via the Meta Pixel. Individually and collectively, these impact whether and what data a developer can send via the Meta Pixel, demonstrating that Mr. Zeidman’s conclusion that “the Meta Pixel operated in a largely uniform manner”¹⁹⁹ is not only unsupported but is also wrong.

1. Users Can Employ Ad Blockers or Other Browser Extensions that Prevent Data Transmissions

84. One factor that creates variability in developers’ transmission of data via the Meta Pixel is that users can install ad blockers or other browser extensions that block certain data transmissions, including those sent to Meta’s servers via the Meta Pixel. For example, Adblock Plus, one of the most used ad blockers that has served more than 60 million users since 2006, has the ability to block data transmissions from specific domains.²⁰⁰ To do so, Adblock Plus relies on

¹⁹⁹ Zeidman Report, ¶ 40.

²⁰⁰ “Meet Adblock Plus: The Original Ad Blocker,” *Adblock Plus*, November 29, 2023, <https://blog.adblockplus.org/blog/meet-adblock-plus-the-original-ad-blocker>, accessed September 25, 2025 (“[Adblock Plus] ha[s] blocked hundreds of millions of ads since then while serving more than 60 million users.”). Ms. Doe testified to using Adblock Plus since as early as 2016 or 2020. Deposition of Jane Doe (“Doe Deposition”), June 24, 2025, at 207:5–17 (“Q. Do you use an ad blocker? A. Yes. Ad Block Plus is the one I currently have. I think I’ve had it for quite a while. [...] Q. Do you have an approximate range in years since you’ve been using Ad Block Plus? A. I feel like I have memories of using it in Indiana. So that would be as early as, like, 2016 or 2020, not that along ago, but probably -- I was probably using some form of Ad Blocker since, I don’t know, 2015 or something.”).

predefined filter lists to block communications.²⁰¹ These lists include the *connect.facebook.net/fbevents.js* URL, which is necessary for the Meta Pixel to function.²⁰² Therefore, enabling Adblock Plus automatically blocks data transmissions via the Meta Pixel.²⁰³ I confirmed this by visiting the H&R Block website with Adblock Plus enabled (see **Figure 12**). Users may also use other browser extensions that function similarly to Adblock Plus, including Facebook Container²⁰⁴ and uBlock Origin.²⁰⁵

²⁰¹ “About Adblock Plus,” *Adblock Plus*, <https://adblockplus.org/en/about>, accessed October 16, 2025 (“Adblock Plus is a free extension that allows you to customize your web experience. You can block annoying ads, disable tracking and lots more. It’s available for all major desktop browsers and for your mobile devices. [...] Choose what you want to see when browsing the web by using filter lists to block unwanted elements, like ads or tracking.”).

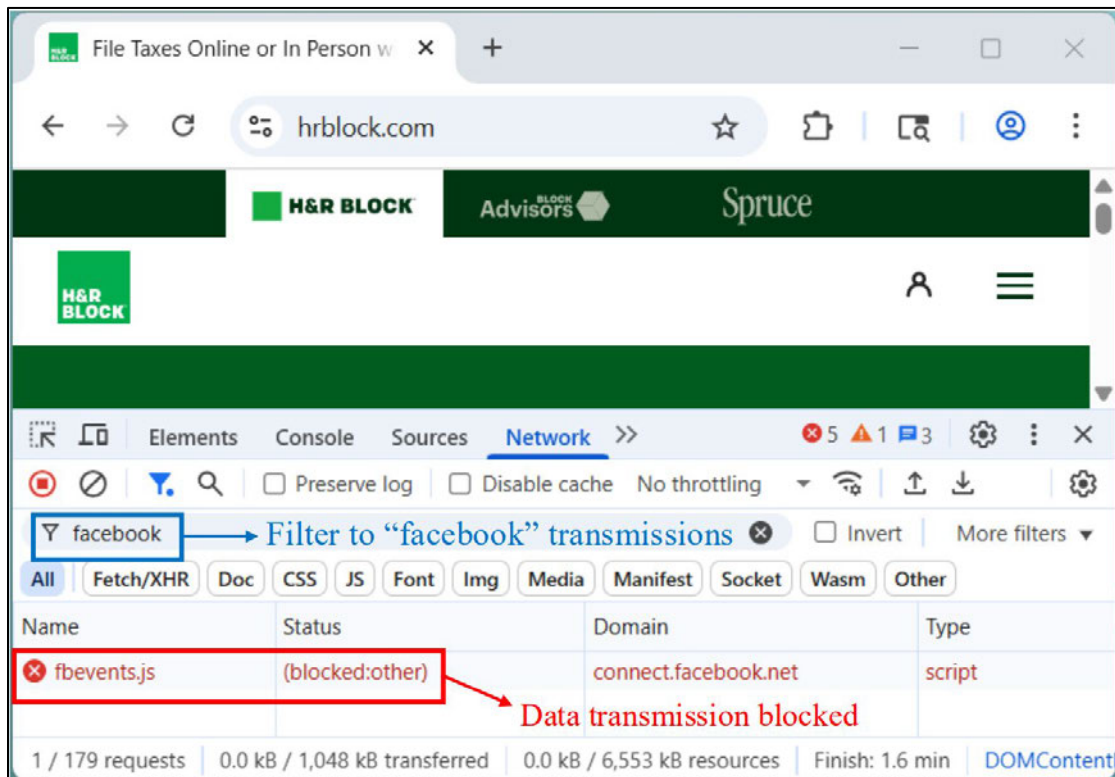
²⁰² See “ABP Filters (Compliance),” *Adblock Plus*, October 20, 2025, <https://easylist-downloads.adblockplus.org/v3/full/abp-filters-anti-cv.txt>, accessed October 26, 2025 (“`||facebook.net^*/fbevents.js$third-party`”).

²⁰³ “ABP Filters,” *Adblock Plus*, October 6, 2025, <https://easylist-downloads.adblockplus.org/abp-filters-anti-cv.txt>, accessed October 6, 2025 (“Filter list designed to fight circumvention ads (including, in some cases, their tracking) and fix critical issues for Adblock Plus users.”); “abp-filters-anti-cv,” *GitLab*, August 3, 2018, <https://gitlab.com/eyeo/anti-cv/abp-filters-anti-cv>, accessed October 20, 2025 (“ABP Anti-Circumvention Filter List is enabled by default in Adblock Plus version 3.1 or higher.”).

²⁰⁴ “Facebook Container - Prevent Facebook from Tracking You on Other Websites,” *Mozilla Support*, June 24, 2025, <https://support.mozilla.org/en-US/kb/facebook-container-prevent-facebook-tracking>, accessed September 15, 2025 (“Facebook Container is a Firefox add-on that helps you set boundaries with Facebook and other Meta websites. This extension isolates Meta sites (including Facebook, Instagram, and Messenger) from the rest of the web to limit where the company can track you.”).

²⁰⁵ “uBlock Origin - Free, Open-Source Ad Content Blocker,” *uBlock Origin*, <https://ublockorigin.com/>, accessed October 16, 2025 (“uBlock Origin is not just an ‘ad blocker’, it’s a wide-spectrum content blocker[.]”).

Figure 12: Data Transmissions from Visit to *hrblock.com* Are Blocked When Adblock Plus Is Equipped on Chrome²⁰⁶



85. Ad blockers are implemented as browser extensions that operate within the environment of a specific browser.²⁰⁷ As such, their functionality depends on the browser and the device on which they are installed.²⁰⁸ If a user changes browsers, reinstalls software, or accesses a website from another device, the ad blocker may not be present or configured in the same way.

²⁰⁶ See **Appendix D**; “windows_chrome_hrblock_abp.har” in my produced backup materials.

²⁰⁷ “Getting Started with Adblock Plus,” *Adblock Plus*, https://adblockplus.org/getting_started, accessed October 16, 2025 (“Adblock Plus is the most popular browser extension available for Mozilla Firefox, Google Chrome, Opera and Android.”); “uBlock Origin - Free, Open-Source Ad Content Blocker,” *uBlock Origin*, <https://ublockorigin.com/>, accessed October 16, 2025 (“The uBlock Origin extension remains an industry leading, open-source, cross-platform browser extension with software developed specifically for multiple platform use[.]”); “Facebook Container - Prevent Facebook from Tracking You on Other Websites,” *Mozilla Support*, June 24, 2025, <https://support.mozilla.org/en-US/kb/facebook-container-prevent-facebook-tracking>, accessed September 15, 2025 (“Facebook Container is a Firefox add-on that helps you set boundaries with Facebook and other Meta websites.”).

²⁰⁸ “About Adblock Plus,” *Adblock Plus*, <https://adblockplus.org/en/about>, accessed October 16, 2025 (“Adblock Plus is a free [web] extension that allows you to customize your web experience. [...] It’s available for all major desktop browsers and for your mobile devices.”); “Why Doesn’t Adblock Work as Well on Mobile Devices?”

86. Browser extensions such as ad blockers can be easily turned on and off, either globally or for specific websites, using “pause” or “allowlist”²⁰⁹ options accessible from the browser.²¹⁰ This means that users can temporarily disable or re-enable blocking without uninstalling the ad blocker extension. Accordingly, data transmissions from the H&R Block and TaxAct websites for website visitors can vary from visitor to visitor and for the same visitor over time, depending on whether users had an ad blocker active at a given time.

87. The use of ad blockers and other browser extensions to block certain data transmissions is not uncommon, and the number of people using ad-blocking software and other browser extensions in the U.S. has grown substantially over time. According to one estimate, “16% of the U.S. online population used ad blockers during Q2 2015.”²¹¹ Another estimate showed 32.2% of U.S. internet users aged 16 to 64 used ad blockers as of Q1 2024.²¹² A 2018 report estimated that

AdBlock, <https://helpcenter.getadblock.com/hc/en-us/articles/9738536045075-Why-doesn-t-AdBlock-work-as-well-on-mobile-devices>, accessed October 16, 2025 (“[M]obile OS ecosystems and browsers prevent us from offering you the same great experience [available on Desktop.]”); “uBlock Origin Works Best on Firefox,” *GitHub*, September 26, 2024, <https://github.com/gorhill/uBlock/wiki/uBlock-Origin-works-best-on-Firefox>, accessed October 16, 2025 (“The Firefox version of uBO uses WebAssembly code for core filtering code paths. With Chromium-based browsers, this is not the case because this would require an extra permission in the extension manifest[.]”).

²⁰⁹ “Pausing and Unpausing AdBlock Using a Keyboard Shortcut or Context Menu Command,” *AdBlock Help Center*, <https://helpcenter.getadblock.com/hc/en-us/articles/9738549326995-Pausing-and-unpausing-AdBlock-using-a-keyboard-shortcut-or-context-menu-command>, accessed October 16, 2025 (“AdBlock [...] allow you to [...] pause or resume ad blocking.”); “Add a Website to the Allowlist,” *AdBlock Plus Help Center*, <https://help.adblockplus.org/hc/en-us/articles/1500002589982-Add-a-website-to-the-allowlist>, accessed October 16, 2025 (“[A]n allowlist is a list of items that has been approved to receive special privileges. You can add website URLs to an allowlist in order to view ads on websites that you want to support.”).

²¹⁰ “Facebook Container - Prevent Facebook from Tracking You on Other Websites,” *Mozilla Support*, June 24, 2025, <https://support.mozilla.org/en-US/kb/facebook-container-prevent-facebook-tracking>, accessed September 15, 2025 (“You can add other websites to Facebook Container, if you prefer Facebook to see your activity on that site. [...] Select Allow Site in Facebook Container at the bottom of the panel.”); “Disable uBlock,” *uBlock Help Center*, <https://support.ublock.org/hc/en-us/articles/37100838523667-Disable-uBlock>, accessed October 16, 2025 (“If a website you are trying to access does not allow ad blockers or if you want to support a content creator via ad revenue, you can easily disable uBlock for a specific website. [...] Click Pause uBlock if you want to disable uBlock for the specific page you are visiting. [...] Click Allow ads on this site if you want uBlock off for the entire website.”).

²¹¹ PageFair and Adobe, “The Cost of Ad Blocking - PageFair and Adobe 2015 Ad Blocking Report,” 2015, p. 3.

²¹² “Ad Blocker Usage and Demographic Statistics in 2024,” *Backlinko*, September 2, 2024, <https://backlinko.com/ad-blockers-users#adblock-by-country>, accessed October 20, 2025.

about 43% of U.S. internet users engage in some form of ad blocking each month.²¹³ Several of the Named Plaintiffs in this matter—Mr. Papadimitriou, Ms. Doe, and Ms. Bryant—testified that they used ad blockers or other browser settings to limit online tracking.²¹⁴ The use of ad blockers and other browser extensions suggests by H&R Block and TaxAct website users would have resulted in data transmissions via the Meta Pixel being blocked—potentially at different times throughout the class periods, even for the same user.

2. *Users Can Grant or Deny Website-Specific Consent for Certain Tracking Technologies*

88. Another factor that creates variability is users’ choices on individual websites. Many websites display consent banners to give users the choice to grant or deny permission for certain data transmissions.²¹⁵ As discussed in **Section III.C**, these technologies can be implemented through tag managers, like those used by the H&R Block and TaxAct websites. If users reject all cookies or accept only those strictly necessary, developers may be prevented from transmitting some or any data via the Meta Pixel. Consent preferences may expire after a designated period of time, depending on the website’s configuration, resulting in potential variation in data transmission

²¹³ Globalwebindex, “Ad-Blocking: A deep-dive into ad-blocking trends,” 2018, p. 6 (“AD-BLOCKING AROUND THE WORLD [...] % of internet users who block ads on any device each month [...] U.S.A. 43%[.]”).

²¹⁴ Deposition of Chris Papadimitriou, Senior Architect at Cprime, (“Papadimitriou Deposition”), June 6, 2025, at 44:1–45:8 (“Q. Do you block search engines from tracking you? A. If I see an option, I typically do. I usually would have an ad blocker in place. Q. What is the name of the ad blocker that you use? A. I think it was just called AdBlock, but I don’t recall. Q. Do you know how long you have used AdBlock? A. [...] Years. I don’t know if it’s enabled on my current computer[.] [...] Q. Do you recall when you first started using AdBlock? A. [...] Roughly the 2000s sometime.”); Doe Deposition, at 43:8–14 (“Q. You mentioned you block some ads. Is there a service or software that you use to block ads? A. Yeah. I have ad blocker on all the time, unless, like, there’s a particular website that I need and it forces me to turn it off.”), at 207:5–18 (“Q. Do you use an ad blocker? A. Yes. [...] Q. When did you start using Ad Block Plus? [...] I was probably using some form of Ad Blocker since, I don’t know, 2015 or something.”); Deposition of Tiffany Elizabeth Bryant, July 21, 2025, at 63:22–24 (“Q. When did you start using -- or have you used Adblock Plus? A. Yes.”).

²¹⁵ Habib, Hana, at el., “‘Okay, Whatever’: An Evaluation of Cookie Consent Interfaces,” *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI ’22)* 621, 2022, p. 1 (“When consumers visit a website for the first time, their experience is often interrupted with an interface related to the use of cookies. These interfaces, used to meet legal requirements for notice and consent to data collection[.]”).

to Meta over time, even for a given user.²¹⁶ For example, Ms. Doe and Mr. Papadimitriou testified that they managed cookie and privacy settings—such as clearing cookies, turning off tracking, or opting out of targeted ads—which would have prevented or limited data transmissions from their visits to the H&R Block and TaxAct websites if they set their cookie and privacy settings to prevent the transmission of data.²¹⁷

89. Furthermore, visitors to *hrblock.com* with an IP address associated with California are presented with a consent banner that allows them to grant or deny the use of “targeted advertising technologies” as seen in **Figure 13**. In such cases, data transmissions to *connect.facebook.net* or *facebook.com* do not take place unless a user clicks “Accept,” or alternatively clicks on “Customize Settings” and opts in to the use of “Non Service Provider” tools, and then refreshes the site or navigates to another page on the site (see **Figure 14**).²¹⁸ A user can also click “Decline” or click the “X” in the top right corner to close the consent pop-up, either of

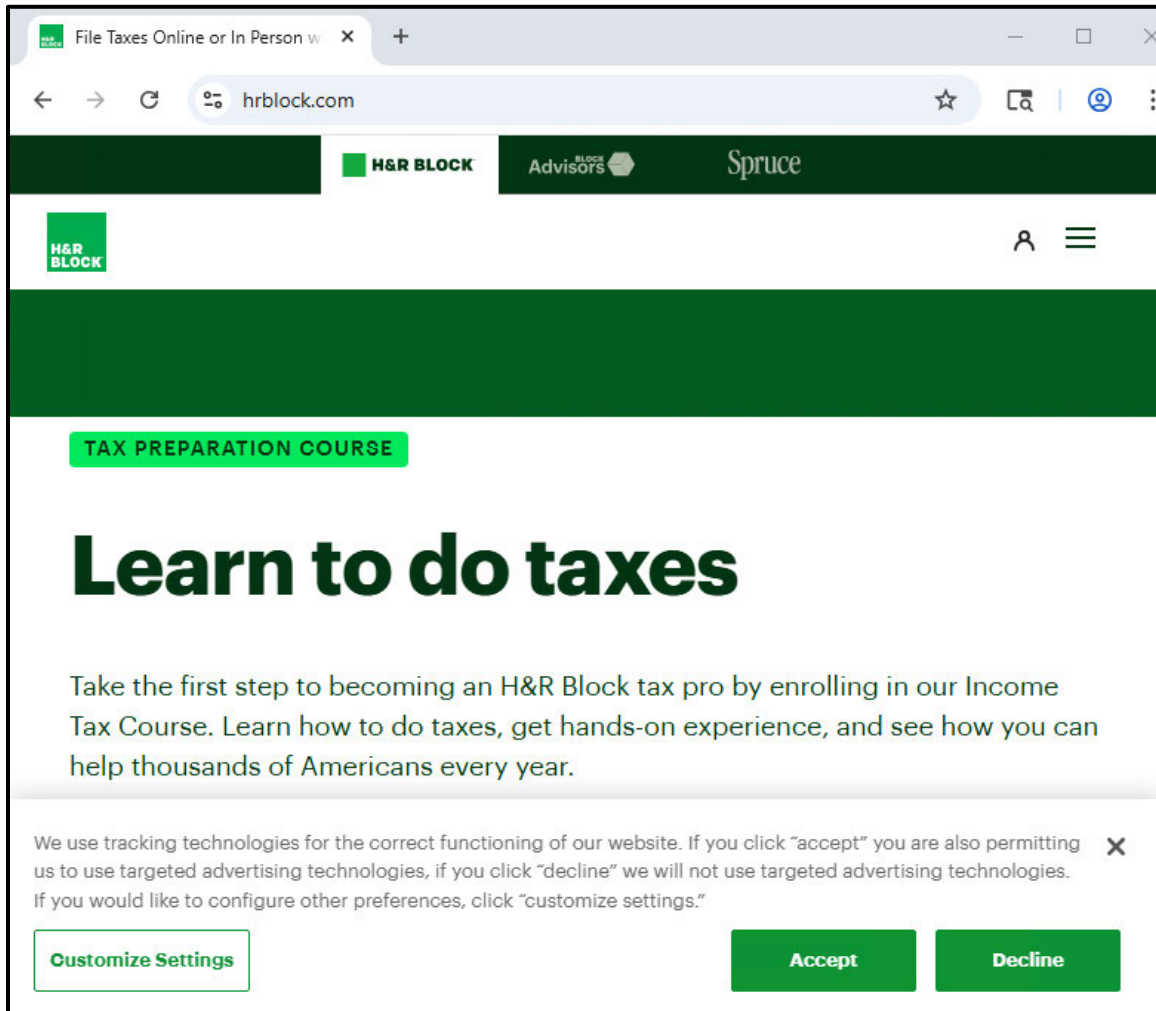
²¹⁶ “What Is Cookie Consent? Requirements and Tools to Comply with Global Data Privacy Law,” *Cookiebot*, May 8, 2024, <https://www.cookiebot.com/en/cookie-consent/>, accessed September 16, 2025 (“A cookie consent banner [...] appears on websites when a user first visits, if they’ve cleared their browser settings, or if a legally required expiry of previous consent has passed.”); “Understanding Cookie Consent Expirations,” *Syrenis*, April 22, 2024, <https://syrenis.com/resources/blog/understanding-cookie-consent-expirations/>, accessed September 16, 2025 (“Website and cookie policies [...] [W]ebsites set their expiration period for cookie categories opted for by users. Usually, websites set them to expire anything between hours or days to last as long as months or even years.”).

²¹⁷ Doe Deposition, at 33:6–34:4 (“Q. Have you taken any steps to protect your online privacy? A. Yes. Q. What steps have you taken? A. [...] what I do all the time in every situation on every device or things like that, but I do things like turn off cookies, even though it’s very annoying and I have to do multiple steps for sign in [...] but I turn off cookies, turn off the browsing history, have it so it doesn’t save it at all. [...] I turn off all history-type things, generally. I don’t have cookies on whenever possible. Every time a website does the cookies pop-up, I -- I click and do the minimum and only the required cookies. And I just am careful about what I share.”); Papadimitriou Deposition, at 41:4–15 (“Q. [...] Have you taken any other steps to protect your online privacy? [...] A. My personal browser clears cookies and everything whenever I’m done for the day or whenever I close it. [...] Q. You mentioned you set the settings on [Firefox] browser to clear cookies. A. Yeah.”).

²¹⁸ See **Appendix D**; “windows_chrome_hrblock_default.har,” “windows_chrome_hrblock_default_noRefresh.har” in my produced backup materials.

which prevents the transmission of any data via the Meta Pixel.²¹⁹ If the user provides consent, the developer can start sending data via the Meta Pixel during the user’s next visit to the website.

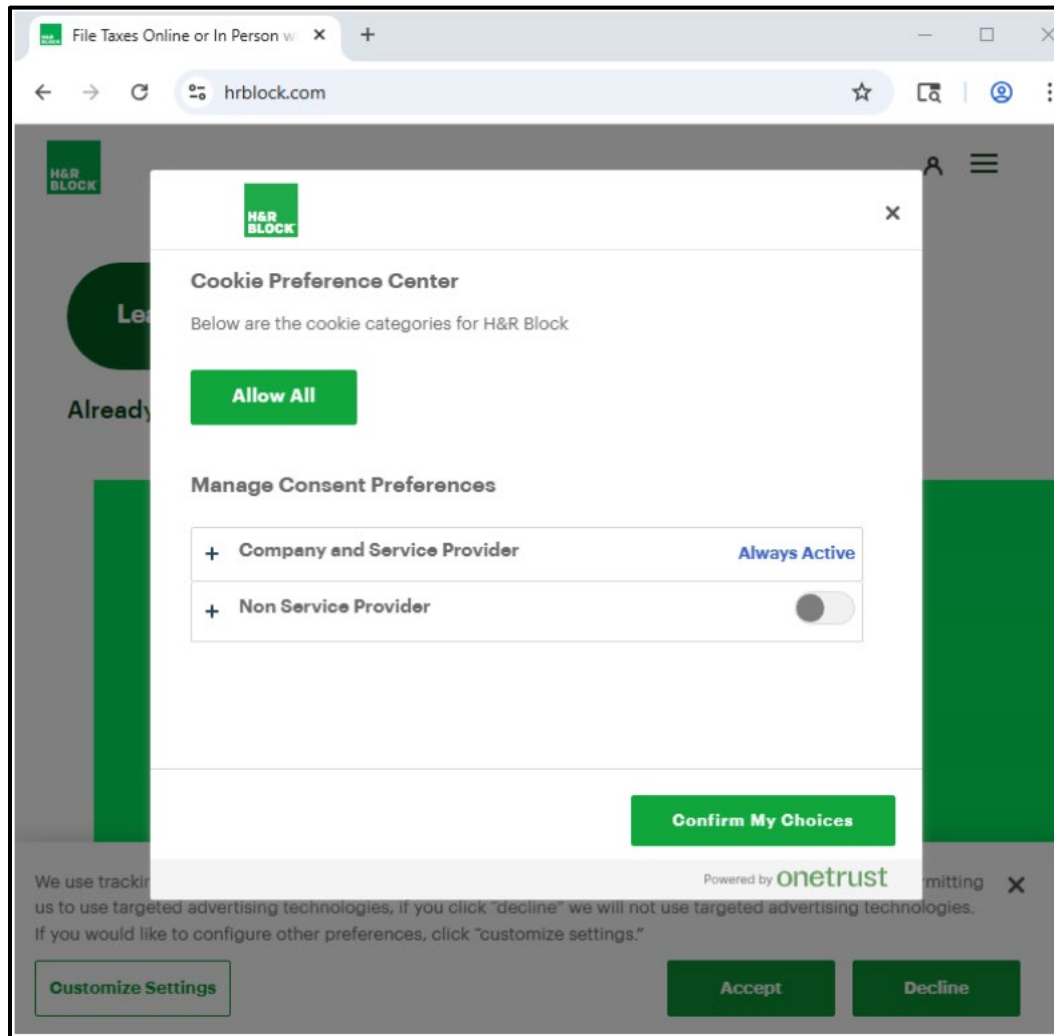
Figure 13: Cookie Consent Banner Presented to *hrblock.com* Users with California-Based IP Addresses²²⁰



²¹⁹ See **Appendix D**; “windows_chrome_hrblock_rejectSiteConsent.har” in my produced backup materials.

²²⁰ “File Taxes Online or In-Person,” *H&R Block*, <https://www.hrblock.com/>, accessed October 22, 2025.

Figure 14: Cookie Preferences Menu Available to hrblock.com Users with California-Based IP Addresses²²¹



90. Consent banners were present on *hrblock.com* and *blockadvisors.com* for some but not all of the proposed class periods, demonstrating Mr. Zeidman’s claim that “the Meta Pixel operated in a largely uniform manner” across both websites during the proposed class periods is wrong.²²²

91. Though *taxact.com* does not automatically display a consent banner when users visit the TaxAct website, users can navigate to *taxact.com/do-not-sell-or-share* to opt out of “Targeting

²²¹ “Cookie Preference Center,” *H&R Block*, <https://www.hrblock.com/>, accessed October 22, 2025.

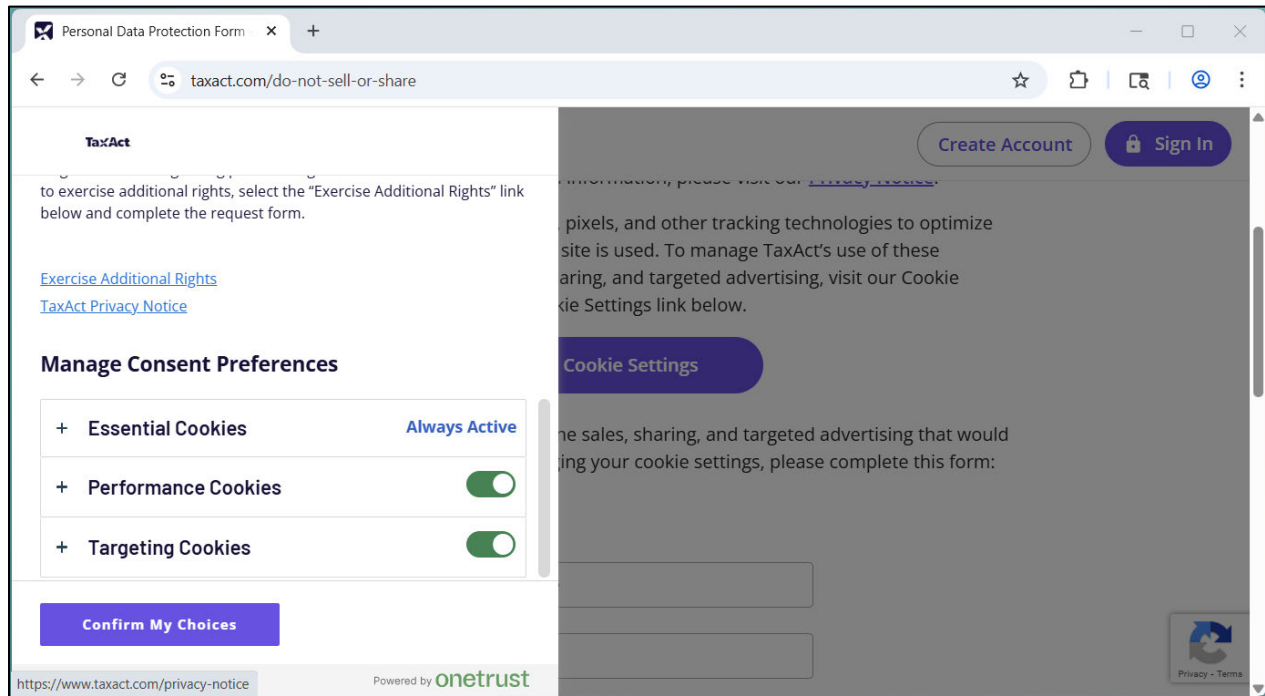
²²² Appendix D; Section III.C.

Cookies” as seen in **Figure 15**. Once a user opts out, the Meta Pixel is disabled and developers cannot transmit any data via the Meta Pixel.^{223, 224} According to my analysis of historical versions of *taxact.com* using Wayback Machine, consent banners have been in place at least since January 2023.²²⁵ Whether users need to revisit *taxact.com/do-not-sell-or-share* to maintain their opt-out of “Targeting Cookies” status over time depends on how the TaxAct website configures cookie lifespan and whether those cookies persist across devices and browsing sessions. A user’s need to revisit *taxact.com/do-not-sell-or-share* to maintain their opt-out of “Targeting Cookies” status is another source of potential variation in data transmission to Meta over time, even for a given user.

²²³ “Opt Out of Sales, Sharing and Targeted Advertising,” *TaxAct*, <https://www.taxact.com/do-not-sell-or-share>, accessed October 20, 2025 (“TaxAct, and our partners, use cookies, pixels, and other tracking technologies to optimize your experience and analyze how our site is used. To manage TaxAct’s use of these technologies and opt out of selling, sharing, and targeted advertising, visit our Cookie Preference Center by clicking the Cookie Settings link below.”).

²²⁴ See **Appendix D**; “windows_chrome_taxact_rejectSiteConsent.har” in my produced backup materials.

²²⁵ See **Appendix D**; **Section III.C**.

Figure 15: Cookie Preferences Menu Available to *taxact.com* Users with California-Based IP Addresses²²⁶

3. *Users Could Have Previously Visited a Meta Domain or Can Be Logged In to a Meta User Account, Affecting Cookie Transmission*

92. An additional factor that creates variability in data transmitted via the Meta Pixel is users’ previous interactions with Meta. The specific cookies that Meta sets in a user’s browser, which may subsequently be transmitted as a result of developer’s use of the Meta Pixel, depend on the user’s prior interactions with Meta domains, as shown in **Figure 16** below. Users who have never interacted with a Meta domain will have no Meta-specific third-party cookies, and consequently, no such third-party cookies will be included in data transmissions via the Meta Pixel. Users who have visited Meta domains but are not logged into Facebook will not have the *c_user*

²²⁶ “Opt Out of Sales, Sharing and Targeted Advertising / Cookie Preferences,” *TaxAct*, <https://www.taxact.com/do-not-sell-or-share>, accessed October 25, 2025.

cookie present in their browser, and consequently, this cookie will not be included in any data transmitted via the Meta Pixel.²²⁷

Figure 16: Cookies Stored on Users’ Browsers from Prior Interactions with *facebook.com* Based on Site Visit to *hrblock.com*²²⁸

Prior Interactions with <i>facebook.com</i>	Third-Party Meta Cookies
No Interactions with <i>facebook.com</i>	
Visit <i>facebook.com</i> (Not Logged In)	<i>datr, dpr, fr, sb</i>
Visit <i>facebook.com</i> (Logged In)	<i>c_user, datr, fr, sb, xs</i>

93. In contrast, users logged into Facebook may have all relevant third-party cookies (*c_user, datr, fr, sb, xs*) present in their browser. If such a user subsequently visits a website where the developer has integrated the Meta Pixel, then these third-party cookies would be included in that developer’s data transmissions to Meta’s servers unless the user has taken an action to disable the transmission of third-party cookies or prevent the functionality of the Meta Pixel entirely (see **Section VII.A.2**). Users’ previous interactions with Meta domains can vary from user to user, so whether and which cookies were transmitted for H&R Block and TaxAct website users may have varied across users and over time. This, too, is contrary to Mr. Zeidman’s claim that “the Meta Pixel operated in a largely uniform manner” across both websites during the proposed class periods.

²²⁷ “Cookies Policy,” Meta Privacy Center, [https://www.facebook.com/privacy/policies/cookies?annotations\[0\]=explanation%2F1_common_cookies_and_users](https://www.facebook.com/privacy/policies/cookies?annotations[0]=explanation%2F1_common_cookies_and_users), accessed October 27, 2205 (“*c_user*; *xs* [...] We use these cookies to authenticate [a user] and keep [the user] logged in as [they] navigate between Facebook Pages.”).

²²⁸ See **Appendix D**; “*windows_chrome_hrblock_noLogin*,” “*windows_chrome_hrblock_noActiveLogin*,” and “*windows_chrome_hrblock_default*” in my produced backup materials. Additional third-party Meta cookies may be stored on the user’s browser. I list the third-party Meta cookies present in my testing.

4. *Users Can Adjust Browser-Specific Controls or Use Browsers that Affect What Data Can Be Sent Via the Meta Pixel*

94. Users’ ability to block certain cookies or types of cookies is another reason why data transmission is not uniform for all users. Modern browsers, such as Chrome,²²⁹ Mozilla Firefox,²³⁰ and Safari,²³¹ have a variety of settings that allow users to modify how the browsers operate, including the ability to block certain cookies or types of cookies. Mr. Zeidman did not consider this type of variation when claiming data transmission is “uniform.”

95. Whether first- and third-party cookies are created and transmitted may vary depending on the user’s browser and browser settings. Browsers such as Firefox (see **Figure 17**) and Safari (see **Figure 18**) block third-party cookies by default in regular browsing mode. In these

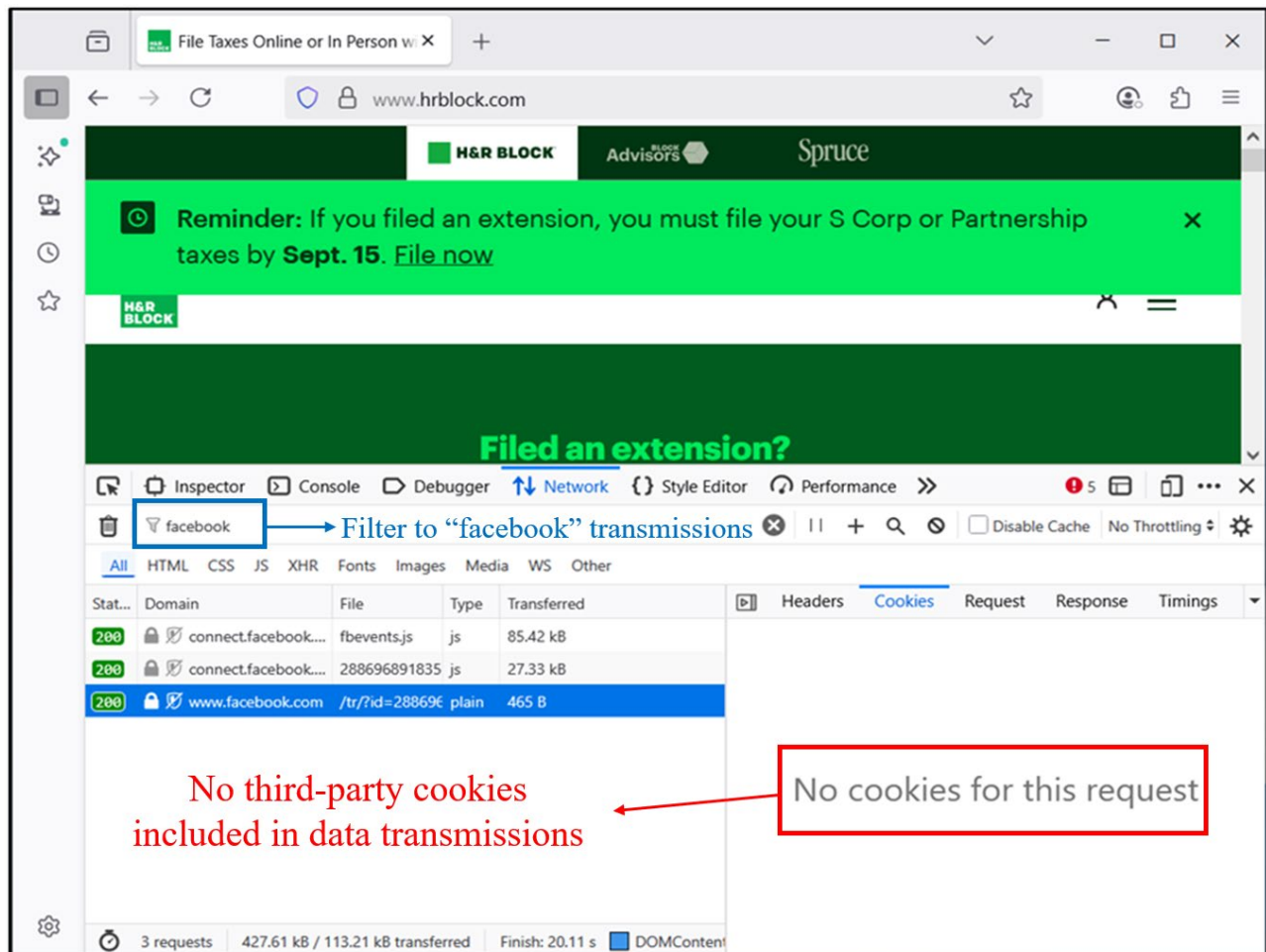
²²⁹ On March 1, 2010, Chrome introduced a range of privacy settings that let users, among other things, control whether websites can store cookies. *See* Mazor, Orit, “Windows Beta Update: Translate and Content Controls,” *Chrome*, March 1, 2010, <https://chromereleases.googleblog.com/2010/03/windows-beta-update-translate-and.html>, accessed October 20, 2025 (“More content settings to let you control whether web sites can store cookies, load images, use plug-ins, run JavaScript or show pop-ups.”). *See also*, Gilbertson, Scott, “Google Chrome Beta Adds Privacy and Content Controls,” *Wired*, March 2, 2010, <https://www.wired.com/2010/03/google-chrome-beta-adds-privacy-and-content-controls/>, accessed September 30, 2025 (“The new features allow for much more fine-grained control of cookies, images, JavaScript, plug-ins, and pop-up windows, allowing you to always block them, always allow them or only allow them from trusted sites [...] If you elect to disable cookies (or any of the other options) Chrome will display an icon in the URL bar which you can click to add an exception.”).

²³⁰ In 2006, Mozilla Firebird (the predecessor to Firefox) introduced improved privacy options, including a one-click feature to clear all cookies and an advanced preferences panel with cookie whitelisting through the new “Cookie Exceptions” window. *See* “Mozilla Firebird 0.6 - Release Notes,” *Firefox*, December 6, 2013, https://website-archive.mozilla.org/www.mozilla.org/firefox_releasenotes/en-us/firefox/releases/0.6, accessed September 30, 2025 (“Improved Privacy Options [...] With a single click (and a confirmation) you can clear all privacy data including form data, history, cache, cookies, etc”). *See also*, “Mozilla Firebird 0.7 - Release Notes,” *Firefox*, December 6, 2013, https://website-archive.mozilla.org/www.mozilla.org/firefox_releasenotes/en-us/firefox/releases/0.7, accessed October 20, 2025 (“Cookie whitelisting (through the new Cookie Exceptions window)”).

²³¹ As of 2018, all major browsers (Google Chrome, Apple Safari, Microsoft Edge, and Mozilla Firefox) allowed users to set up their cookie preferences. *See* Nield, David, “How to Lock Down What Websites Can Access on Your Computer,” *Wired*, November 4, 2018, <https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/>, accessed October 23, 2025 (“Apple Safari Privacy Settings[:] [...] Use the Block all cookies checkbox to stop all websites from saving all cookies, although this might prevent some sites from functioning correctly. More granular control is available via the Manage Website Data button: The subsequent dialog box lets you clear cookies from particular sites, or clear all the cookies that are saved on your laptop in one go.”).

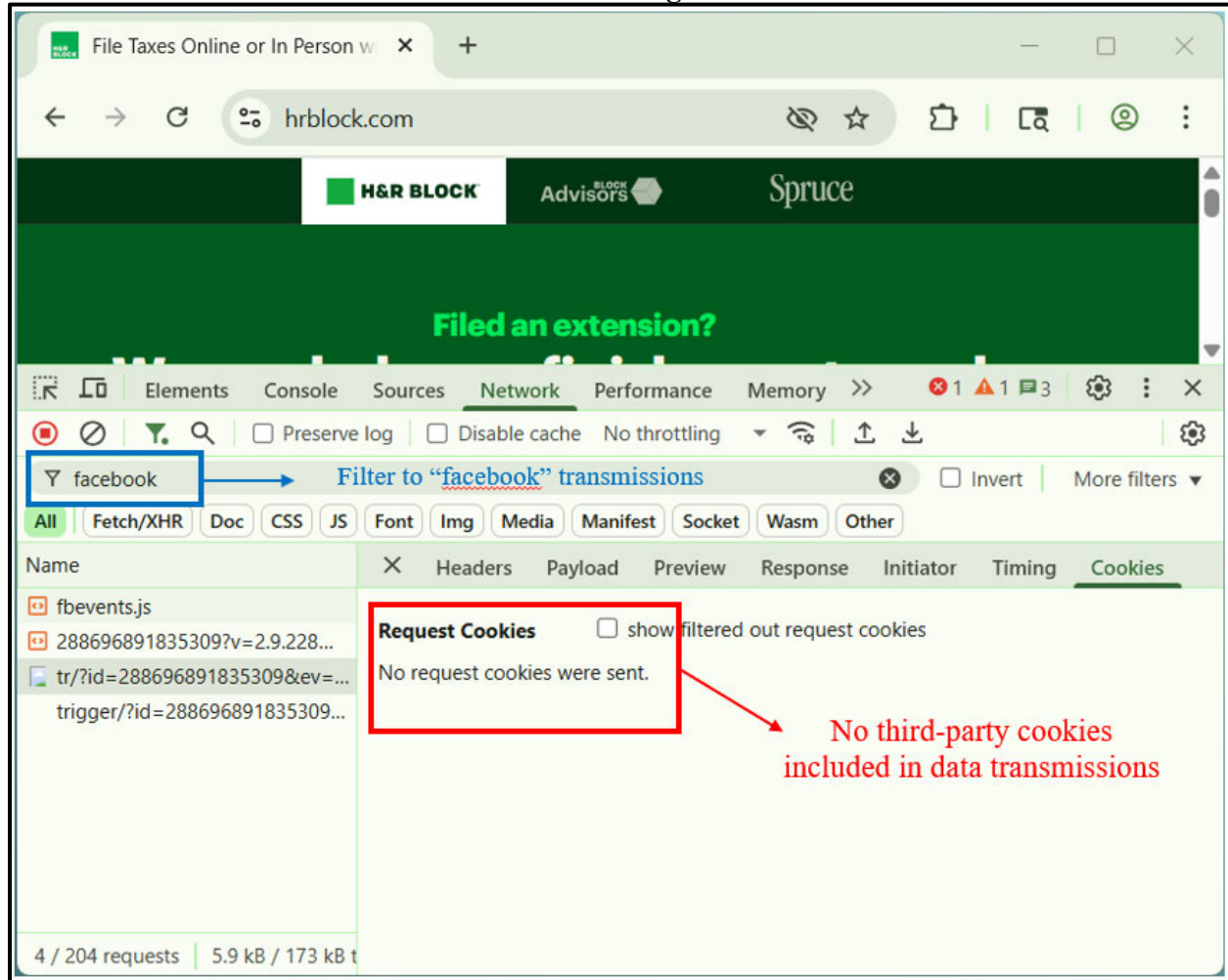
instances, developers can still transmit data via the Meta Pixel but cannot include third-party cookies—such as *c_user*, *datr*, and *fr*—which impacts Meta’s ability to link visits to individual Meta user accounts.

Figure 17: No Third-Party Cookies Are Associated with a Data Transmission from Visit to *hrblock.com* Using Firefox²³²



²³² See Appendix D; “windows_firefox_hrblock_default.har” in my produced backup materials.

Figure 18: No Third-Party Cookies Are Associated with a Data Transmission from Visit to *hrblock.com* Using Safari²³³



96. Though Chrome allows both first- and third-party cookies in regular browsing mode by default, users can choose to block third-party cookies, as shown in **Figure 19**.²³⁴ Only the first-party *fbp* cookie value is transmitted when third-party cookies are blocked.²³⁵ The value of the *fbp*

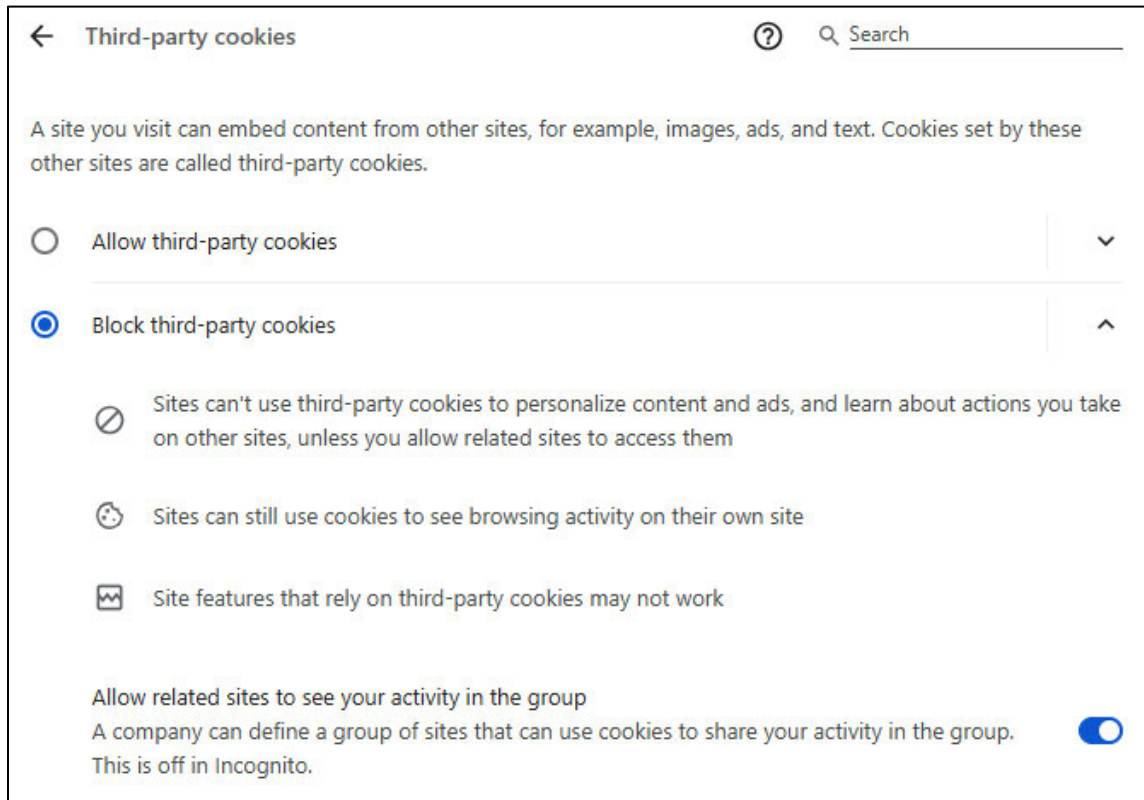
²³³ See **Appendix D**; “mac_safari_hrblock_default.har” in my produced backup materials.

²³⁴ I find that choosing to block third-party cookies in Chrome prevents the transmission of third-party cookies to Meta upon a site visit to *hrblock.com*. See **Appendix D**; “windows_chrome_hrblock_block3p.har” in my produced backup materials.

²³⁵ “Delete, Allow and Manage Cookies in Chrome,” *Google Chrome Help*, <https://support.google.com/chrome/answer/95647>, accessed September 22, 2025 (“In Incognito mode, third-party cookies are blocked by default.”).

cookie contains a random number and is not shared across websites a user visits.²³⁶ This illustrates that even in browsers where some cookies are transmitted, individual users’ choices impact what cookie-based information is sent to Meta.²³⁷

Figure 19: Chrome Third-Party Cookie Blocking Settings



²³⁶ “ClickID and the fbp and fbc Parameters,” *Meta*, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/>, accessed September 15, 2025 (“The fbp event parameter value must be of the form version.subdomainIndex.creationTime.randomnumber[.]”).

²³⁷ Mr. Zeidman’s and Mr. Weir’s methodologies do not account for the possibility that data on user interactions with the H&R Block and TaxAct websites may potentially remain unmatched to users or possibly matched to users who did not actually take the action associated with the event data. My review of the fields

5. *Users Can Visit Websites with Strict or Private Browsing Modes that Block the Transmission of Data via the Meta Pixel*

97. Most browsers offer private or incognito browser modes, which do not retain browser history and delete cookies and web cache data when the user session ends.²³⁸ Chrome Incognito mode also blocks third-party cookies by default.²³⁹ Additionally, certain browsers, including Firefox and Safari, offer browsing modes that enforce “strict” tracking prevention, limiting the transmission of data to third parties. It is common for browsers in their private browsing sessions to enable by default some or all of the components involved in “strict” tracking prevention configurations.²⁴⁰ Ms. Doe and Mr. Papadimitriou testified to using such private or incognito browser modes to limit online data transmission.²⁴¹

²³⁸ Bodnar, Danielle, “What Is Private Browsing?,” *Norton*, June 28, 2024, <https://us.norton.com/blog/privacy/what-is-private-browsing>, accessed September 22, 2025 (“Private browsing is a feature in most web browsers that lets you browse the internet without leaving a record of your activity on your device.”). *See, e.g.*, “How Chrome Incognito Keeps Your Browsing Private,” *Google Chrome Help*, <https://support.google.com/chrome/answer/9845881>, accessed September 22, 2025 (“Incognito mode can help keep your browsing private from other people who use your device.”).

²³⁹ “Delete, Allow and Manage Cookies in Chrome,” *Google Chrome Help*, <https://support.google.com/chrome/answer/95647>, accessed September 22, 2025 (“In Incognito mode, third-party cookies are blocked by default.”).

²⁴⁰ *See, e.g.*, “Enhanced Tracking Protection in Firefox for Desktop,” *Mozilla Support*, <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>, accessed September 16, 2025 (“Tracking content: These trackers are hidden in ads, videos and other in-page content. In Standard mode, tracking content is blocked only in Private Windows. To add this protection to all windows, visit your privacy preferences and select Strict or Custom as explained below.”); “Privacy,” *Apple*, <https://www.apple.com/privacy/features/>, accessed October 20, 2025 (“Safari protects your privacy automatically. Private Browsing adds even more protections. When it’s activated, Safari won’t add the sites you visit to your history, remember your searches, or save any information from forms you fill out online — and advanced tracking and fingerprinting protections go even further to help prevent websites from tracking or identifying your device. Known trackers are completely prevented from loading on pages, and link tracking protection removes tracking added to URLs as you browse. Content blocker support is designed so that it can’t send developers information about what you’re looking at. And private browsing windows automatically lock — requiring your device password to be unlocked — when you’re not using them.”).

²⁴¹ Papadimitriou Deposition, at 42:9–21 (“Q. Do you ever or have you ever used hidden or incognito modes? A. Yes. [...] Q. What search -- what other browsers have you used incognito or hidden mode on? A. Usually, I would use Chrome for work, use Safari the odd time on my phone is what the default is for the iPhone. And then I’ve tried Microsoft Edge.”); Doe Deposition, at 36:16–23 (“Q. [...] Have you ever used Incognito mode? A. Oh, yes, a lot of times. I haven’t been doing it lately, but I have done that a lot. [...] Q. Do you use Incognito mode on your phone browser? A. I have, yes.”).

98. Firefox uses the open-source Disconnect filter list to block certain domains when in “strict” mode.²⁴² As shown in **Figure 20**,²⁴³ strict mode blocks social media trackers, cross-site cookies, and tracking content, among other web tools.²⁴⁴ When this mode is enabled, all requests to *connect.facebook.net* are blocked, preventing the transmission of data via the Meta Pixel. **Figure 21** demonstrates an example of this, showing what happens when the H&R Block website is opened in a Firefox browser operating in “strict” mode. Strict mode identifies the *fbevents.js* script, a Meta Pixel script used by the H&R Block website to transmit event data, as a “Socialtracking” request, and keeps the script from being loaded. Such tracking protections are also enabled by default in Firefox users’ private browsing sessions.²⁴⁵

²⁴² “Shavar-prod-lists,” *Mozilla Services*, <https://github.com/mozilla-services/shavar-prod-lists>, accessed September 16, 2025 (“Firefox’s Enhanced Tracking Protection features rely on lists of trackers maintained by Disconnect.”).

²⁴³ “Shavar-prod-lists,” *Mozilla Services*, <https://github.com/mozilla-services/shavar-prod-lists>, accessed September 16, 2025 (“Firefox consumes the list as follows: Tracking: anything in the Advertising, Analytics, Social, Content, or Disconnect category. Firefox ships two versions of the tracking lists: the ‘Level 1’ list, which excludes the ‘Content’ category, and the ‘Level 2’ list which includes the ‘Content’ category.”); “Enhanced Tracking Protection in Firefox for Desktop,” *Mozilla Support*, <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>, accessed September 16, 2025 (“Strict Enhanced Tracking Protection. This will block the following: [...] Tracking content in all windows.”).

²⁴⁴ By default, Firefox’s private browsing mode applies the same tracking prevention as Strict mode, enforcing the full Disconnect blocklists. This blocks all embedded third-party content from domains identified by Disconnect as tracking domains, including the Meta Pixel. *See* “Enhanced Tracking Protection in Firefox for Desktop,” *Mozilla Support*, <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>, accessed September 16, 2025 (“Standard Enhanced Tracking Protection. By default, Firefox blocks the following on all sites: [...] Tracking content in Private Windows only.”).

²⁴⁵ “Enhanced Tracking Protection in Firefox for Desktop,” *Mozilla Support*, <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>, accessed September 16, 2025 (“Tracking content: These trackers are hidden in ads, videos and other in-page content. In Standard mode, tracking content is blocked only in Private Windows. To add this protection to all windows, visit your privacy preferences and select Strict or Custom as explained below.”)

Figure 20: Browsing Modes Available to Firefox Users²⁴⁶

☐ **Standard**
Balanced for protection and performance. Pages will load normally.

☒ **Strict**
Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in all windows
- Cryptominers
- Known and suspected fingerprinters

☒ Allow Firefox to automatically apply exceptions required to avoid major website breakage.

☐ Also apply exceptions automatically that are only required to fix minor issues and make convenience features available.

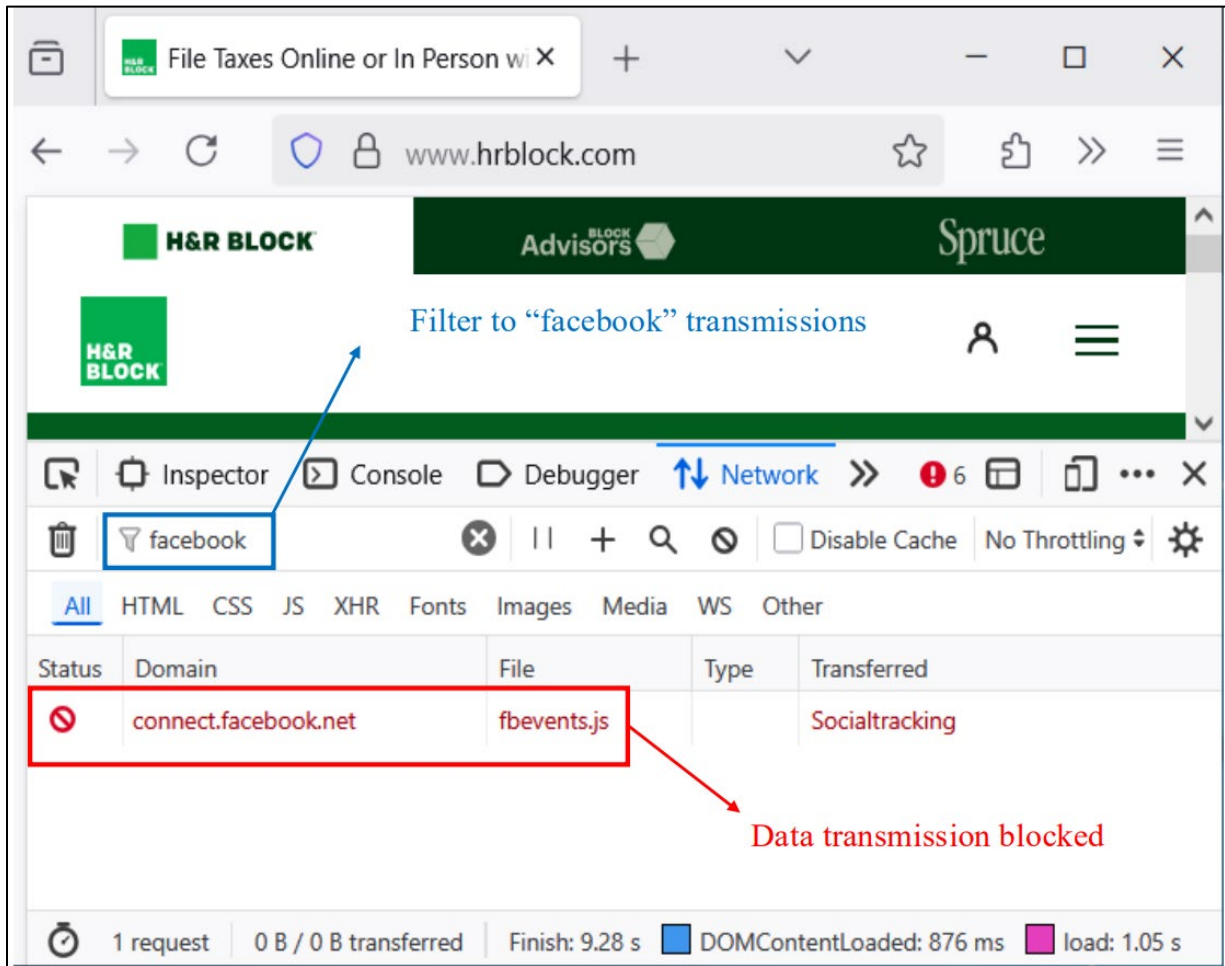
ⓘ You will need to reload your tabs to apply these changes. [Reload All Tabs](#)

⚠ Heads up!
This setting may cause some websites to not display content or function correctly. We provide optional exceptions for websites that we know can be affected by your configuration. To reduce the chance of broken websites, allow these tracker exceptions. If a site appears broken, you can turn off tracking protection for that site to load all content and report the issue so we can help fix it for everyone. [Learn how](#)

☐ **Custom**
Choose which trackers and scripts to block.

²⁴⁶ The Enhanced Tracking Protection settings can be accessed by opening the Firefox menu by clicking the three horizontal lines in the top-right corner. From the dropdown, select Settings, then go to Privacy & Security and find Enhanced Tracking Protection.

Figure 21: Data Transmissions from Visit to *hrblock.com* Are Blocked When Strict Browsing Mode Is Enabled Using Firefox²⁴⁷



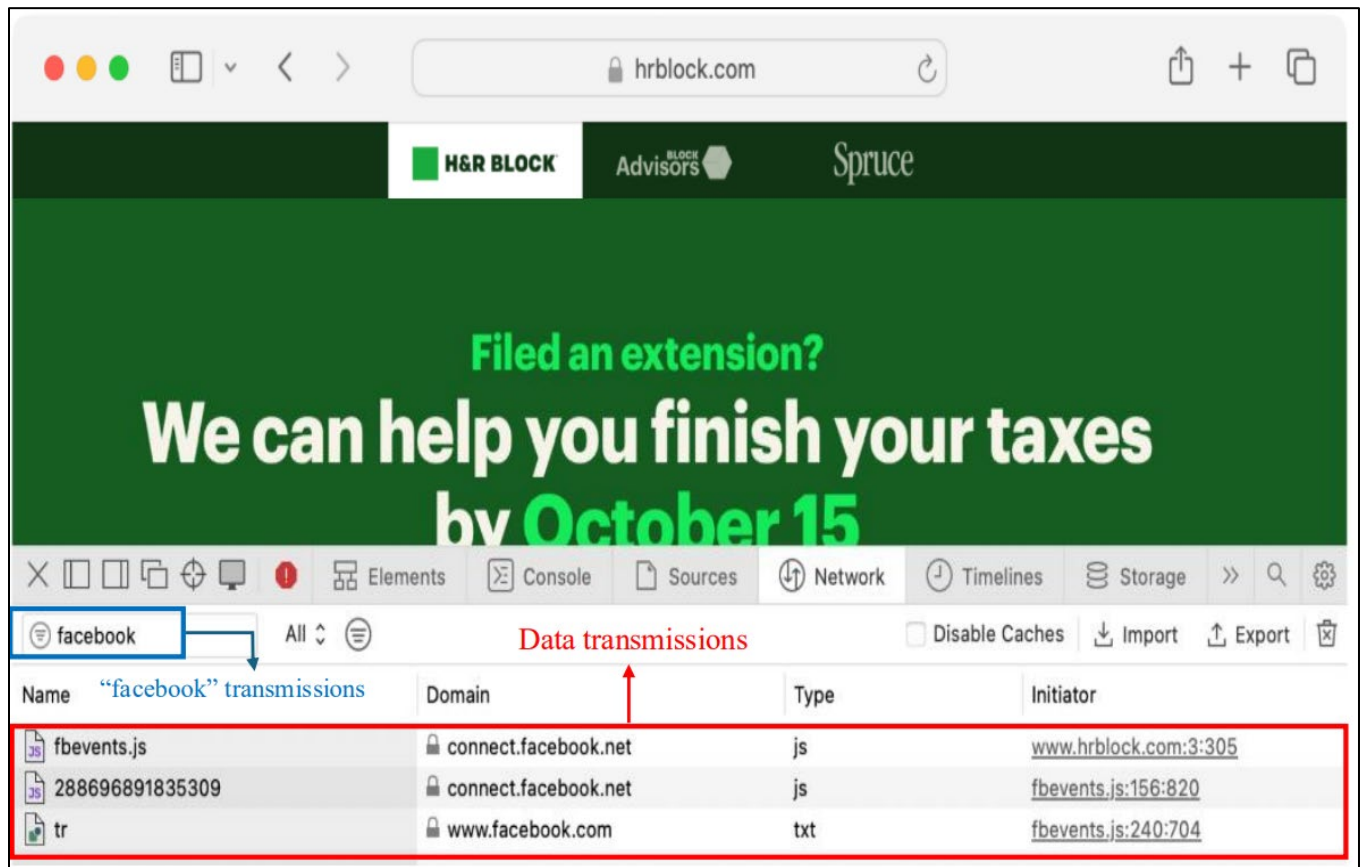
99. Similarly, Safari users can enable “Advanced Tracking and Fingerprinting Protection” (“ATFP”), which blocks network requests to certain domains.²⁴⁸ ATFP is enabled by

²⁴⁷ See **Appendix D**; “windows_firefox_hrblock_strictMode.har” in my produced backup materials.

²⁴⁸ This functionality is enabled by default in Safari’s private browsing mode. See Wilander, John, Charlie Wolfe, Matthew Finkel, Wenson Hsieh, and Keith Holleman, “Private Browsing 2.0,” *WebKit*, July 16, 2024, <https://webkit.org/blog/15697/private-browsing-2-0/>, accessed September 16, 2025. See also, “Easy Privacy,” EasyList, September 16, 2025, <https://easylist.to/easylist/easyprivacy.txt>, accessed September 16, 2025; “DuckDuckGo’s Tracker Blocklists,” *GitHub*, <https://github.com/duckduckgo/tracker-blocklists>, accessed September 16, 2025.

default when browsing in private mode using Safari.²⁴⁹ When AFTP is enabled, requests to *connect.facebook.net* are blocked, preventing the transmission of data via the Meta Pixel, but when AFTP is not enabled, requests to *connect.facebook.net* are not blocked. This can be seen in **Figure 22** and **Figure 23**.

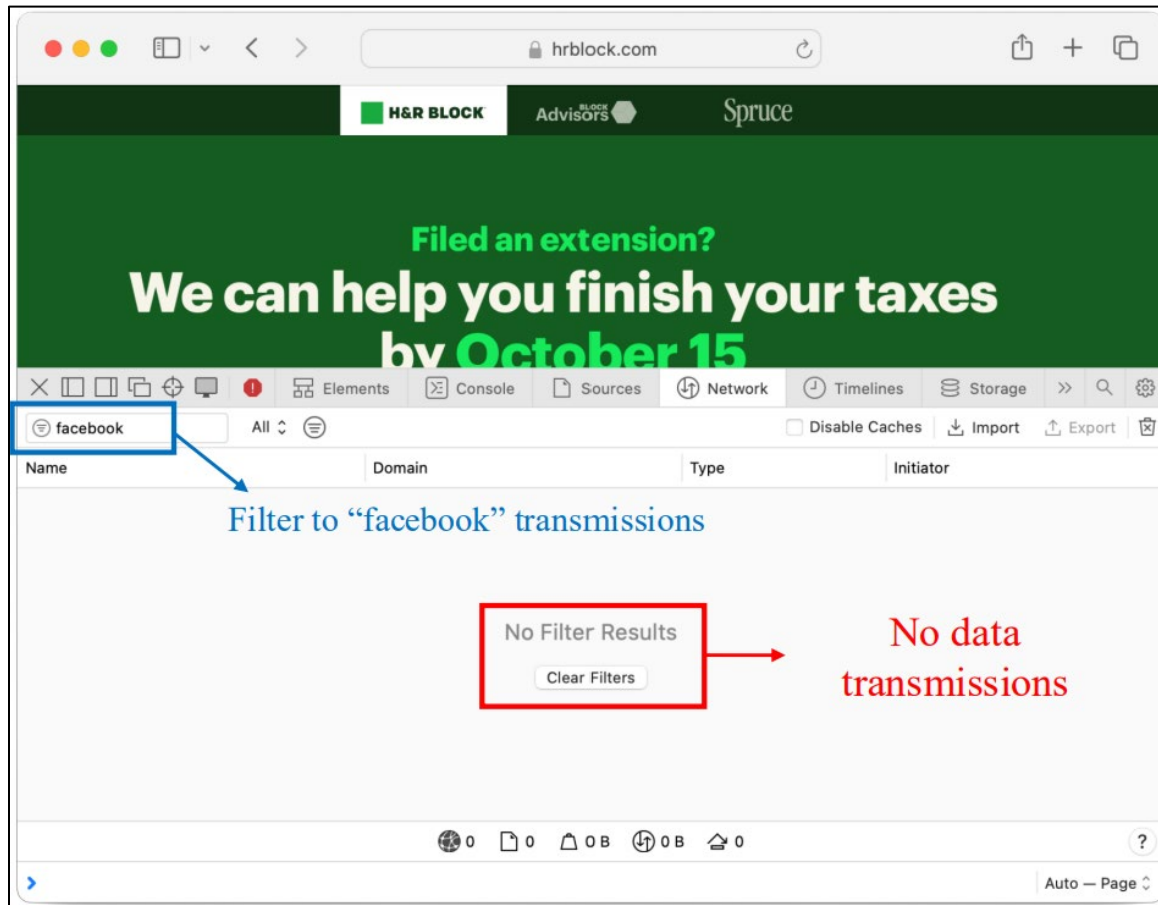
Figure 22: Data Transmissions from Visit to *hrblock.com* Using Safari²⁵⁰



²⁴⁹ “Privacy,” *Apple*, <https://www.apple.com/privacy/features/>, accessed October 20, 2025 (“Safari protects your privacy automatically. Private Browsing adds even more protections. When it’s activated, Safari won’t add the sites you visit to your history, remember your searches, or save any information from forms you fill out online — and advanced tracking and fingerprinting protections go even further to help prevent websites from tracking or identifying your device. Known trackers are completely prevented from loading on pages, and link tracking protection removes tracking added to URLs as you browse. Content blocker support is designed so that it can’t send developers information about what you’re looking at. And private browsing windows automatically lock — requiring your device password to be unlocked — when you’re not using them.”).

²⁵⁰ See **Appendix D**; “mac_safari_hrblock_default.har” in my produced backup materials.

Figure 23: No Data Transmissions from Visit to *hrblock.com* Using Safari with ATFP Enabled²⁵¹



100. Private and strict browsing modes users can choose to use, along with user-enabled tracking protections, can introduce variability in whether and what types of data are transmitted to Meta via the Meta Pixel.

B. Developers Have Controls That Limit or Modify the Data They Can Transmit Via the Meta Pixel, and the TaxAct and H&R Block Websites Used Those Controls in Ways that Affected Their Transmission of Data

101. The choices that developers make about configuring the Meta Pixel affect what data is transmitted to Meta. The Meta Pixel did not “operate in a largely uniform manner” across the

²⁵¹ See **Appendix D**; “mac_safari_hrblock_ATFP.har” in my produced backup materials.

TaxAct and H&R Block websites.²⁵² For instance, developers can choose when and what event data is generated and sent. Because developers control what event data to create and transmit to Meta and when, for what types of users, and from which webpages—and they can change their configuration over time—the event data the H&R Block and TaxAct websites sent to Meta could have varied across users and over time, including for a given user.

102. As discussed in **Section III.C**, when integrating the Meta Pixel through a tag manager, developers have various configuration options that affect data transmissions. For example, developers can take into account user consent by configuring a CMP or other consent mechanisms.

103. I understand that logs associated with the TaxAct website’s and the H&R Block website’s use of the Meta Pixel through their respective tag managers were produced in this matter.²⁵³ Based on my review of these logs, I found evidence that the H&R Block and TaxAct websites configured the Meta Pixel through their tag managers in ways that would have made the Meta Pixel not operate uniformly.²⁵⁴ In this section, I provide illustrative examples demonstrating this.

²⁵² Zeidman Report, ¶ 40 (“During the relevant class periods the Meta Pixel operated in a largely uniform manner on the Tax Preparers’ websites with respect to the basic mechanics of collecting and transmitting visitor data to Meta.”).

²⁵³ See, e.g., TaxAct_00053-0845; HRB_PIXEL_CP218_000000001-5; HRB_PIXEL_CP257_000000002-6; HRB_PIXEL_CP257_000000001.

²⁵⁴ In my analysis of logs, I rely on my professional experience and publicly available documentation describing Adobe Tag Manager configurations. Adobe Tag Manager documentation includes a page specifically dedicated to implementing the Meta Pixel functionality. See “Meta Pixel Extension Overview,” *Adobe Experience League*, <https://experienceleague.adobe.com/en/docs/experience-platform/tags/extensions/client/meta/overview>, accessed October 26, 2025. Adobe Tag Manager operates as a rule-based system, where execution of code—such as the Meta Pixel—depends on conditions defined by developers. A rule consists of an event (the trigger) and an action (what happens once the event occurs). Developers can also specify additional conditions that further limit when a rule executes. For example, a developer may configure the Meta Pixel to trigger when a user performs a specific action but not when the user is browsing in Internet Explorer. See “Rules,” *Adobe Experience League*, <https://experienceleague.adobe.com/en/docs/experience-platform/tags/ui/rules>, accessed October 26, 2025.

1. Developers Choose Whether to Send Events and Parameters to Meta

104. Contrary to Mr. Zeidman’s claims, the Meta Pixel equipped on the TaxAct website was not configured to operate uniformly throughout the proposed class periods with respect to the event data that developers programmed the website to generate and send to Meta. The TaxAct website used both the Google Tag Manager and the Conversant Tag Manager.²⁵⁵ I reviewed the TaxAct tag configuration data, which Mr. Zeidman did not consider,²⁵⁶ and identified examples of TaxAct developers configuring tags to no longer transmit certain information. In November 2022, TaxAct developers added tag manager configuration to stop sending 10 custom parameters that Mr. Zeidman focused on in his report and in his deposition testimony,²⁵⁷ more than six months before the end of the proposed TaxAct class periods. As shown in and **Figure 24** below, I observe that as of November 10, 2022, these parameters are configured to be transmitted. However, all but one, “return_year,” are no longer configured to be transmitted as of November 16, 2022 as shown in **Figure 25**. I observe that “return_year” is configured to not be transmitted as of November 30, 2022.²⁵⁸

²⁵⁵ TaxAct_00384–394 at 385 (“TaxAct used Conversant Tag Manager from 2012 until on or about December 12, 2017, when it completed a transition to Google Tag Manager, the tag management tool currently in use.”).

²⁵⁶ Zeidman Deposition, at 138:4–7 (“Q. Did you review anything that might be considered a tag manager log in connection with this case? A. Not that I recall.”).

²⁵⁷ These parameters are: age range (“age_range”), return year (“return_year”), adjusted gross income (“agi”), federal revenue (“federal_revenue”), federal amount owed (“federal_owe_amount”), federal refund amount (“federal_refund_amount”), number of dependents (“num_of_dependents”), number of standard deductions (“standard_deduction”), state revenue (“state_revenue”), and tax form used (“tax_form”). *See* Zeidman Report, ¶ 49.

²⁵⁸ *See* TaxAct_00097, line 5471; TaxAct_00170.

Figure 24: Select Parameters TaxAct Developers Configured to Be Transmitted to Meta November 10, 2022²⁵⁹

```

<script>
fbq('trackCustom', 'Efile-Print', {
  age_range: '{{DL - Online - age_range}}',
  student_loan_interest: '{{DL - Online - student_loan_interest}}',
  f1099misc: '{{DL - Online - 1099MISC}}',
  ad_tracking: '{{DL - Online - adtracking}}',
  promo: '{{DL - Online - promo}}',
  source_code: '{{DL - Online - source_code}}',
  start_vintage: '{{DL - Online - start_vintage}}',
  customer_type: '{{DL - Online - customer_type}}',
  return_year: '{{DL - Online - return_year}}',
  start_edition: '{{DL - Online - start_edition}}',
  current_edition: '{{DL - Online - current_edition}}',
  start_product_id: '{{DL - Online - start_product_id}}',
  current_product_id: '{{DL - Online - current_product_id}}',
  start_actual_price: '{{DL - Online - start_actual_price}}',
  start_default_price: '{{DL - Online - start default price}}',
  agi: '{{DL - Online - agi}}',
  app_step: '{{DL - Online - app_step}}',
  audit_revenue: '{{DL - Online - audit_revenue}}',
  charitable_contribution: '{{DL - Online - charitable_contributions}}',
  complete_vintage: '{{DL - Online - complete_vintage}}',
  federal_revenue: '{{DL - Online - federal_revenue}}',
  federal_owe_amount: '{{DL - Online - federal owe amount}}',
  federal_refund_amount: '{{DL - Online - federal_refund amount}}',
  filing_status: '{{DL - Online - filing_status}}',
  investments: '{{DL - Online - investments}}',
  modules_submitted: '{{DL - Online - modules_submitted}}',
  mortgage_interest: '{{DL - Online - mortgage interest}}',
  num_of_dependents: '{{DL - Online - number_of_dependents}}',
  payment_type: '{{DL - Online - payment_type}}',
  rpt_revenue: '{{DL - Online - rpt_revenue}}',
  schedule_c: '{{DL - Online - schedule_c}}',
  schedule_c_ez: '{{DL - Online - schedule_c-ez}}',
  software_revenue: '{{DL - Online - software_revenue}}',
  standard_deduction: '{{DL - Online - standard_deduction}}',
  state_revenue: '{{DL - Online - state_revenue}}',
  svc_revenue: '{{DL - Online - svc_revenue}}',
  tax form: '{{DL - Online - tax form}}',
  total_revenue: '{{DL - Online - total_revenue}}',
  w2: '{{DL - Online - w2}}',
});
</script>

```


Figure 25: Select Parameters TaxAct Developers Configured to Be Transmitted to Meta November 16, 2022²⁶⁰

```
<script>
fbq('trackCustom', 'Efile-Print', {
  ad_tracking: '{{DL - Online - adtracking}}',
  promo: '{{DL - Online - promo}}',
  source_code: '{{DL - Online - source_code}}',
  start_vintage: '{{DL - Online - start_vintage}}',
  customer_type: '{{DL - Online - customer_type}}',
  return_year: '{{DL - Online - return_year}}',
  start_edition: '{{DL - Online - start_edition}}',
  current_edition: '{{DL - Online - current_edition}}',
  start_product_id: '{{DL - Online - start_product_id}}',
  current_product_id: '{{DL - Online - current_product_id}}',
  complete_vintage: '{{DL - Online - complete_vintage}}',
});
</script>
```

2. *Developers Can Disable Transmission of Automatic Events*

105. Since the launch of Automatic Events on May 19, 2017, developers have had the option to disable the transmission of Automatic Events.²⁶¹ Developers can disable Automatic Events either by toggling off the “Track events automatically without code” feature in Event Manager or by doing so programmatically by adding the relevant configuration code `fbq('set', 'autoConfig', false, 'FB_PIXEL_ID')`²⁶² to the Meta Pixel.

²⁵⁹ See TaxAct_00092, line 5596; TaxAct_00170; Zeidman Report, ¶ 49.

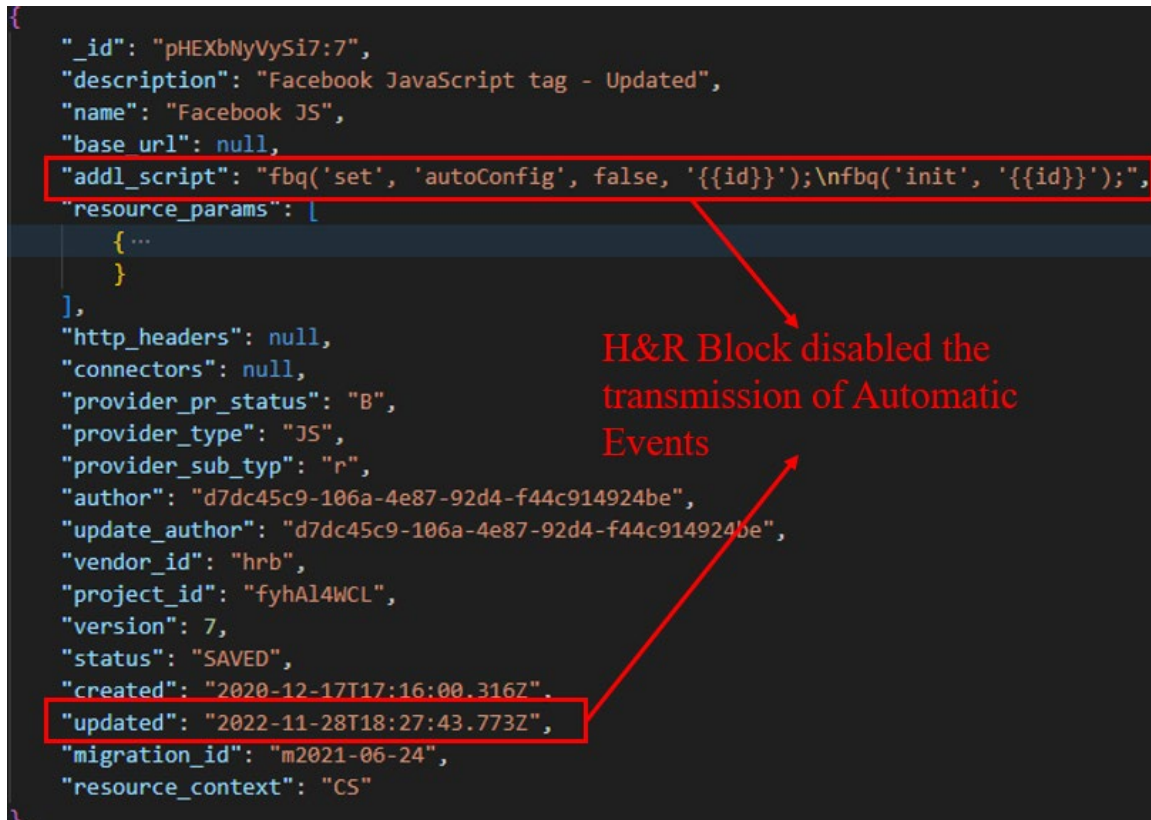
²⁶⁰ See TaxAct_00094, line 5597; TaxAct_00170; Zeidman Report, ¶ 49.

²⁶¹ Facebook for Developers, “Pixel Code Reference,” *Wayback Machine*, as of April 21, 2017, <https://web.archive.org/web/20170421084502/https://developers.facebook.com/docs/facebook-pixel/api-reference>, accessed October 20, 2025 (“Automatic Configuration[:] Starting on May 19, 2017, the Facebook Pixel will be able to send button click data and page metadata from your website to improve your ads delivery and measurement with no further code changes required. If you’d like to configure the Facebook Pixel to Manual Only mode, you can add the line `fbq('set', 'autoConfig', 'false' 'FB_PIXEL_ID')` above the init call in the Facebook Pixel Base code and the Facebook Pixel will no longer send this additional data.”).

²⁶² Facebook, “Pixel Code Reference,” *Wayback Machine*, as of April 21, 2017, <https://web.archive.org/web/20170421084502/https://developers.facebook.com/docs/facebook-pixel/api-reference>, accessed October 20, 2025 (“Automatic Configuration[:] Starting on May 19, 2017, the Facebook Pixel will be able to send button click data and page metadata from your website to improve your ads delivery and measurement with no further code changes required. If you’d like to configure the Facebook Pixel to Manual Only mode, you can add the line `fbq('set', 'autoConfig', 'false' 'FB_PIXEL_ID')` above the init call in the

106. As shown in the tag manager settings produced in this matter (see **Figure 26**), H&R Block developers disabled the transmission of Automatic Events in November 2022 in at least one of the tags present on the site.²⁶³ This setting remains present in the website's code as of today (see **Figure 27**).

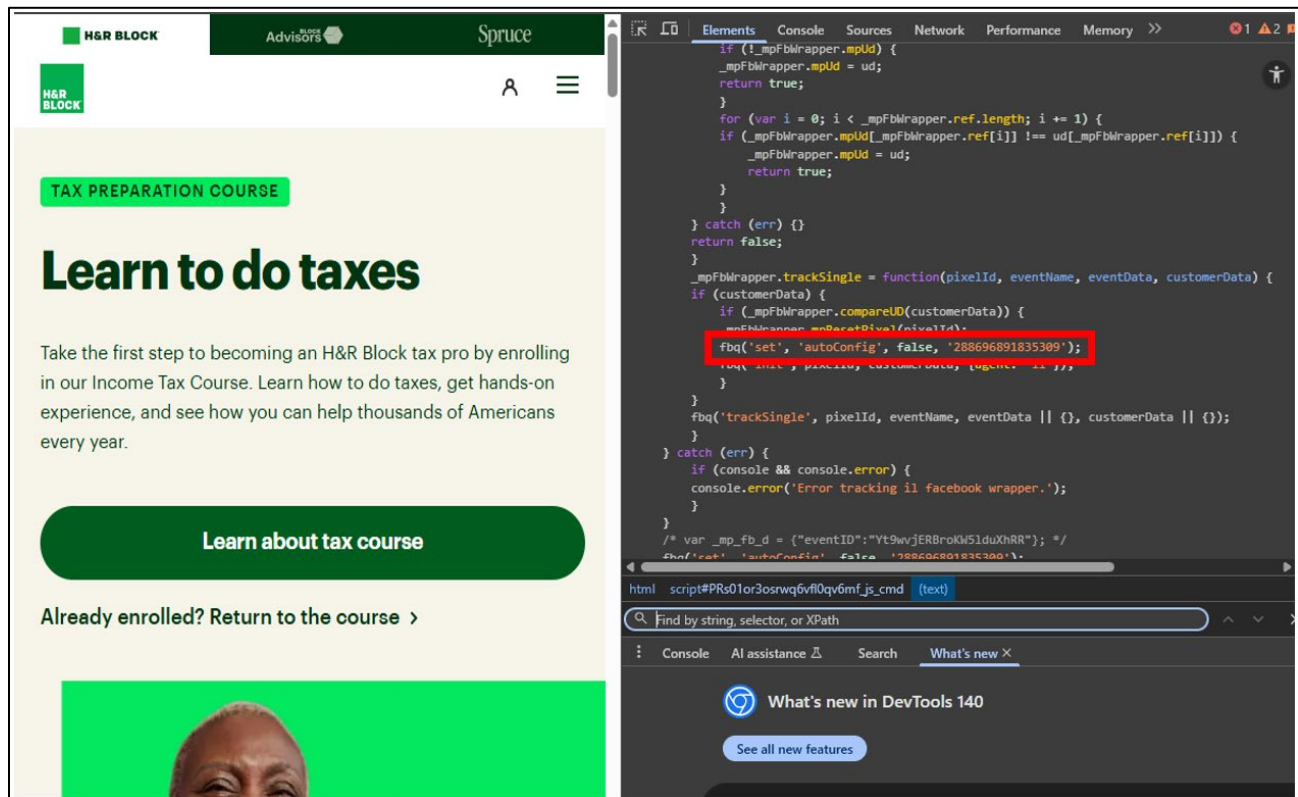
Figure 26: The H&R Website Block Disabled Transmission of Automatic Events in the Tag File Code that Implements the Meta Pixel²⁶⁴



Facebook Pixel Base code and the Facebook Pixel will no longer send this additional data.”). *See also* “Advanced,” *Meta*, <https://developers.facebook.com/docs/meta-pixel/advanced/>, accessed September 29, 2025.

²⁶³ HRB_PIXEL_CP257_000000004.

²⁶⁴ HRB_PIXEL_CP257_000000004.

Figure 27: The H&R Website Block Disabled the Transmission of Automatic Events²⁶⁵

107. In his deposition, Mr. Zeidman “seem[ed] to recall” a decrease in button click data that may be explained by the disabling of automatic events.²⁶⁶ In my analysis of the Pixel Button Clicks data, I observed that while the Pixel Button Clicks data contain close to 180,000 SubscribedButtonClick events associated with the November 26, 2022 date, only 28 events were associated with the January 26, 2023 date. This number decreases through the end of the period for the produced Meta Pixel Button Clicks data (see **Figure 28** below).

²⁶⁵ See **Appendix D**; “windows_chrome_hrblock_default,” which contains the relevant HTML file as text (“VM294.txt”), in my produced backup materials.

²⁶⁶ Zeidman Deposition, at 87:9–15

Figure 28: Observation Counts of the “SubscribedButtonClick” Event in the Meta Pixel Button Clicks Data by Date²⁶⁷



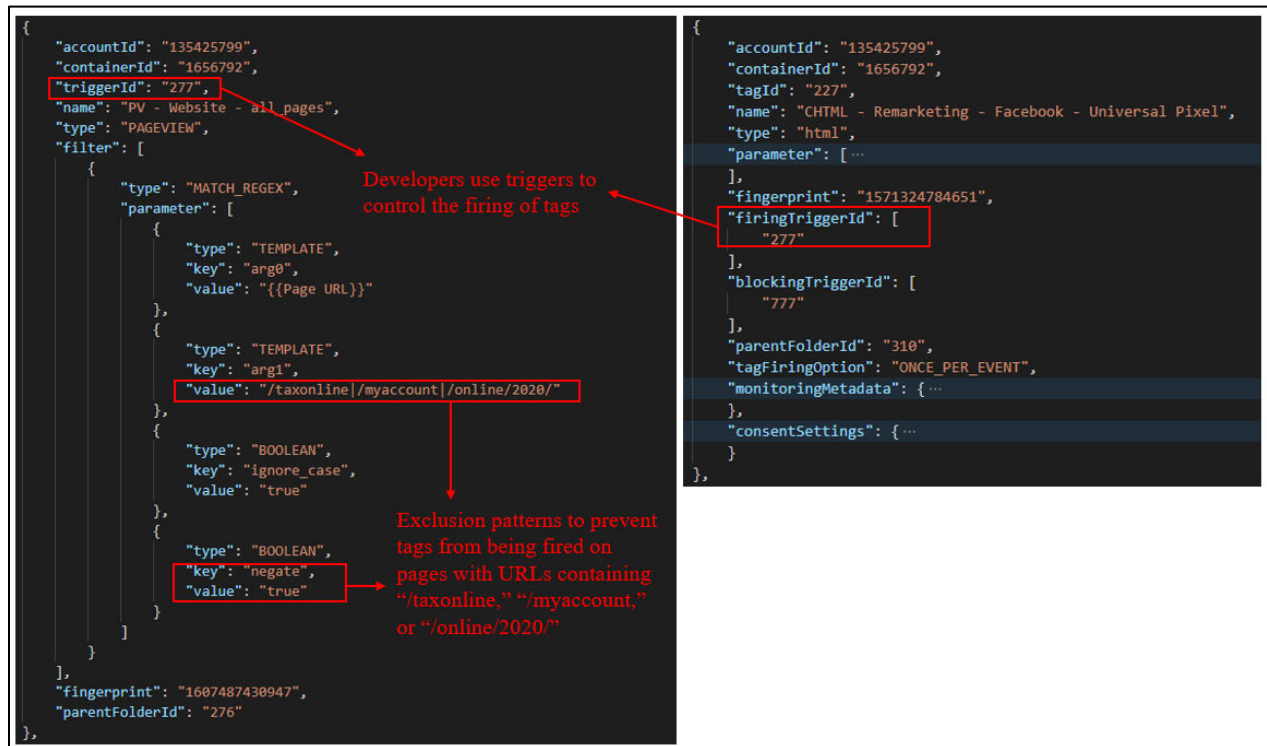
3. *Developers Selected What Webpages Should Generate Events*

108. In addition to configuring what events and event parameters to generate and send, developers can also specify the webpages from which user actions should result in generating event data. In the TaxAct tag configuration data, for example, I observed that on December 17, 2020, certain tags were at that time configured such that certain user actions on webpages with URLs containing “/online/2020,” “/myaccount,” and “/taxonline” would not result in the transmission of events via the Meta Pixel (see **Figure 29** below).²⁶⁸

²⁶⁷ The data is sourced from the field “ds.” I do not include the Inferred Website data in my analysis as it begins in February 2023. See “subscribedbuttonclick_count_by_date” in my produced backup materials.

²⁶⁸ I include this as an illustrative example of configurations made by developers that may affect the behavior of the Meta Pixel over time. It is possible that such configurations were also in place before December 17, 2020.

Figure 29: The TaxAct Website Disabled Transmission of Information on Certain Websites in the Google Tag Manager Container that Implements the Meta Pixel²⁶⁹



4. *Developers Selected the Browsers for Whom to Generate and Send Event Data to Meta*

109. In addition to determining what events and event parameters to generate and send, and from which webpages, developers also control for which browsers event data is generated and sent or not. For example, on October 17, 2019, TaxAct developers introduced a trigger that prevents execution of some of the Meta Pixel integrated on the site from browsers with a User-Agent containing “trident,”²⁷⁰ which corresponds to mobile versions of the Internet Explorer browser.²⁷¹ According to the documentation, this configuration would have blocked the generation and

²⁶⁹ See TaxAct_00495, lines 1402–34, 133541–76; TaxAct_00170.

²⁷⁰ See TaxAct_00684, lines 98241–87; TaxAct_00170.

²⁷¹ See, e.g., “Trident User Agent,” *WhatIsMyBrowser*, https://explore.whatismybrowser.com/useragents/explore/layout_engine_name/trident/, accessed September 30, 2025.

transmission of event data to Meta for users accessing the TaxAct website from the mobile versions of the Internet Explorer browser, thus creating an additional source of variability in data transmission.

110. Additionally, developers can configure event data generation and transmission only for users that meet specific conditions. For example, on January 4, 2018, the TaxAct website configured Google Tag Manager to generate and send the “federal_owe_amount” parameter via the Meta Pixel only when the e-filing status was “success” and the value of the “federal resubmit” choice was “no.”²⁷² For users who did not meet such criteria—*e.g.*, for whom e-filing failed—such data would not be generated or sent. By filtering out the data transmission from users who did not meet these conditions, TaxAct developers added an additional layer of variability in how developers transmitted data to Meta via the Meta Pixel during the TaxAct class period.

111. In short, Mr. Zeidman ignored a number of reasons why developers’ configurations could have affected what information (if any) was sent for each individual user and webpage, including how those configurations changed over time.

C. Meta’s Detection and Filtration Code Varied Over Time

112. As discussed in **Section III.E**, Meta implemented several technical measures to limit or prevent the transmission and receipt of potentially sensitive data. These filters and detection mechanisms were implemented and subsequently modified at different points in time during the proposed class periods. For example, based on my review of Meta’s source code, I observed that on November 8, 2021, Meta introduced filters designed to detect and remove certain types of information, such as [REDACTED]²⁷³ The application of these

²⁷² See TaxAct_00827, lines 13909–36, 25784–844, TaxAct_00170.

²⁷³ See, *e.g.*, [REDACTED]
[REDACTED]

filters at different points in time would have introduced variability in what data is filtered, contrary to Mr. Zeidman’s conclusion that “the Meta Pixel operated in a largely uniform manner.”²⁷⁴

VIII. MR. ZEIDMAN IGNORED CONTROLS THAT META PROVIDES TO ITS USERS TO LIMIT META’S USE OF DATA SENT AS A RESULT OF DEVELOPERS’ USE OF THE META PIXEL FOR ADVERTISING PURPOSES

113. In his report, Mr. Zeidman claimed that developers can use the Meta Pixel to “measure visitor interactions and transmit those interactions to Meta for its use in its advertising and analytics systems,”²⁷⁵ but he ignored online behavioral advertising and off-Facebook activity controls that restrict how Meta may attempt to match or apply that data for personalized ad delivery.

114. **Online Behavioral Advertising (“OBA”) Controls:** OBA refers to “the tracking of a consumer’s activities online—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer’s interests.”²⁷⁶ Meta defines OBA data as “[d]ata produced from user activity on a particular computer or device regarding interactions with non-affiliated websites and applications.”

²⁷⁷ For example, the data developers send via the Meta Pixel would constitute OBA data.

115. When users opt out of OBA through tools, such as the Digital Advertising Alliance (“DAA”), Digital Advertising Alliance of Canada (“DAAC”), and European Digital Advertising

²⁷⁴ Zeidman Report, ¶ 40.

²⁷⁵ Zeidman Report, ¶ 31 (“The Meta Pixel is a JavaScript tracking tool that Meta offers website operators so they can embed it in their webpages to measure visitor interactions and transmit those interactions to Meta for its use in its advertising and analytics systems.”). *See also*, Zeidman Report, ¶ 35 (“It records visitor interactions and transmits event data to Meta’s servers for advertising, analytics, and measurement purpose.”).

²⁷⁶ *Federal Trade Commission*, “Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principle,” December 2007.

²⁷⁷ PIXEL_TAX000058883–893 at 884.

Alliance (“EDAA”),²⁷⁸ Meta sets an opt-out cookie in the user’s browser. This OBA opt-out or “oo” cookie remains in effect until it is either cleared by the user or it expires after five years.²⁷⁹

116. Users may use DAA, DAAC, or EDAA controls to opt out when browsing the internet, in addition to mobile device features such as “Limit Ad Tracking” and “App Tracking Transparency” on iOS.²⁸⁰ Users can also opt out of having Meta use OBA data for advertising by changing their “[a]ctivity information from ad partners” setting in Facebook’s user settings.²⁸¹

117. As part of my analysis, I reviewed how OBA opt-out impacted data transmissions via the Meta Pixel on *hrblock.com* (as an example) and observed that OBA opt-out was executed through the DAA. Specifically, I observed that the “oo” cookie is included in transmissions to Meta servers after the user has opted out of OBA (see **Figure 30**).

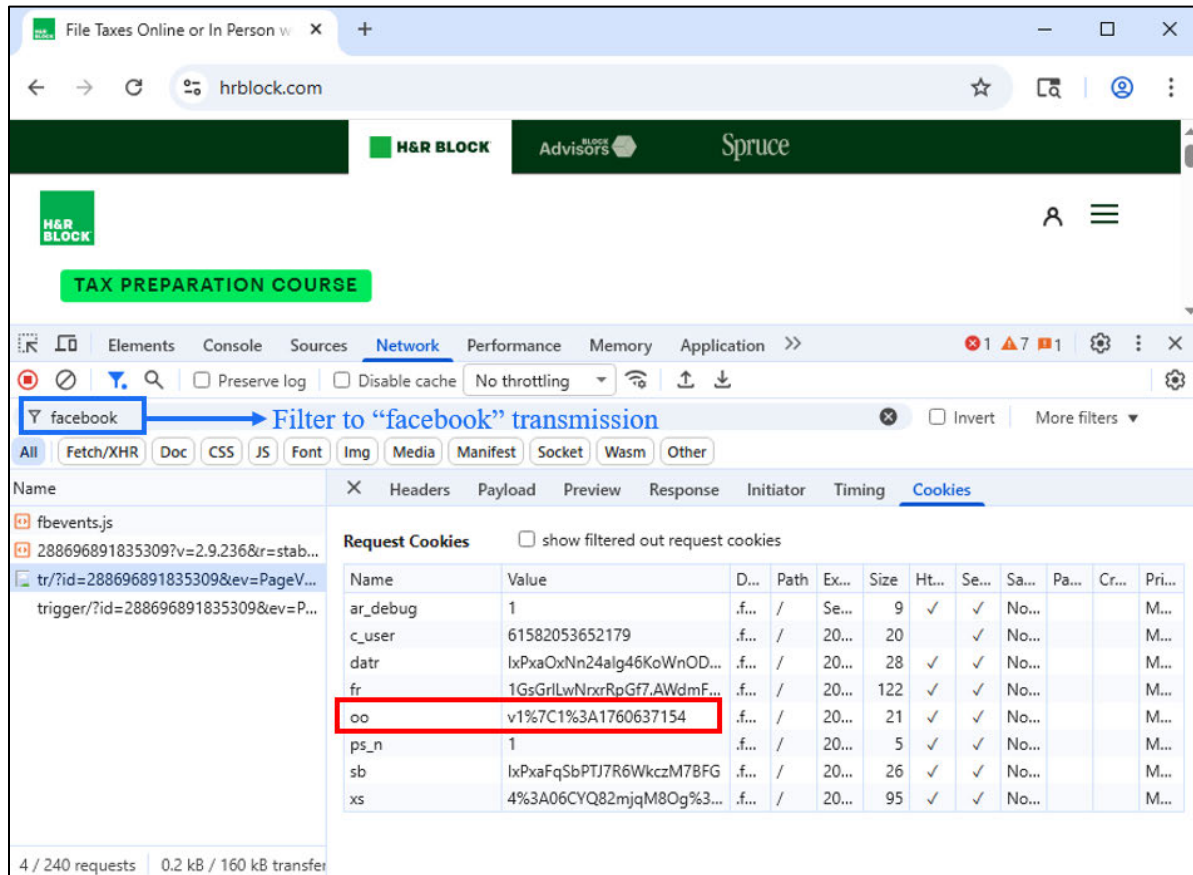
²⁷⁸ PIXEL_TAX000058883–893 at 891 (“We respect the opt-outs a user sets using the Digital Advertising Alliance (DAA), Digital Advertising Alliance of Canada (DAAC), and European Digital Advertising Alliance (EDAA) controls.”).

²⁷⁹ PIXEL_TAX000058883–893 at 891 (“When the user interacts with a toggle on any of the above sites to opt out of online behavioral advertising, we drop an opt out cookie (‘oo cookie’) in the browser. The opt out will be dropped if the user decides to clear their browser cookie. The cookie can otherwise live for up to 5 years.”).

²⁸⁰ “Limited Ad Tracking” was a privacy feature available for mobile devices running on pre-iOS 14 that allowed “iOS users to opt-out of sharing—or effectively having—an Identifier for Advertisers (IDFA)” and receiving “personalized or targeted advertising.” On April 2021, Apple started enforcing “App Tracking Transparency” which no longer shared IDFA by default and “require[d] users to ‘opt-in’ via a prompt to share their IDFA/device ID with an app developer or marketer.” See “What Is Limit Ad Tracking (LAT)?,” *Adjust*, <https://www.adjust.com/glossary/limit-ad-tracking/>, accessed October 26, 2025. See also, “What Is App Tracking Transparency (ATT)?,” *Adjust*, <https://www.adjust.com/glossary/app-tracking-transparency/>, accessed October 25, 2025.

²⁸¹ PIXEL_TAX000058883–893 at 892 (“Users on Facebook can opt out of OBA by visiting their Facebook Ad Settings and modifying the setting marked ‘Ads based on data from partners.’”; “Adjust How Ads on Facebook Are Shown to You Based on Your Activity Information from Ad Partners,” *Meta*, <https://www.facebook.com/help/568137493302217>, accessed October 24, 2025 (“Activity information from ad partners[:] This setting controls whether we can show you relevant ads on Facebook based on information about your Activity information from ad partners. [...] We adhere to the Self-Regulatory Principles for Online Behavioral Advertising and participate in the opt-out programs established by the Digital Advertising Alliance, the Digital Advertising Alliance of Canada and the European Interactive Digital Advertising Alliance.”).

Figure 30: Third-Party Cookies Associated with a Data Transmission from Visit to *hrblock.com* Using Chrome for OBA Opt-Out Users²⁸²



118. When the “oo” cookie is present, Meta does not use the data for personalized ad delivery and instead may use it only for aggregated analytics.²⁸³ Meta verifies a user’s OBA opt-out status twice: first, when it receives data from developers using the Meta Pixel, and second, at

²⁸² See **Appendix D**; “windows_chrome_hrblockOBA.har” in my produced backup materials.

²⁸³ PIXEL_TAX000058883–893 at 891 (“We respect the opt-outs a user sets using the Digital Advertising Alliance (DAA), Digital Advertising Alliance of Canada (DAAC), and European Digital Advertising Alliance (EDAA) controls. These opt-outs can be found at the following websites: DAA: <http://optout.aboutads.info/?c=2&lang=EN>. DAAC: <https://youradchoices.ca/en/tools/>. EDAA: <http://www.youronlinechoices.eu/>. When the user interacts with a toggle on any of the above sites to opt out of online behavioral advertising, we drop an opt out cookie (‘oo cookie’) in the browser. The opt out will be dropped if the user decides to clear their browser cookies. The cookie can otherwise live for up to 5 years.”).

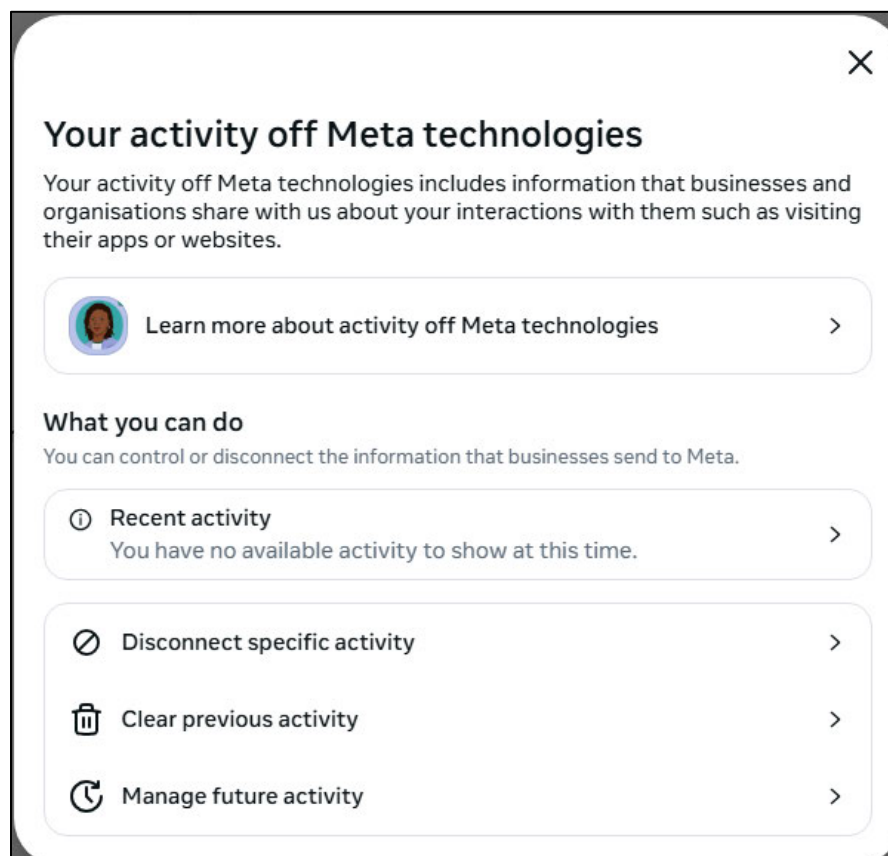
the time of ad delivery. Even if the data is permissible to use, Meta does not use it for personalized ads if the user has opted out by the time of ad delivery.²⁸⁴

119. **Off-Facebook Activity (“OFA”) Controls:** OFA controls allow users to view and manage the data that businesses and organizations share with Meta about their interactions outside of Meta services, including data sent as a result of developers’ use of the Meta Pixel.²⁸⁵ Through these controls, users can “turn off” storage of future matching between their Meta accounts and their activities off Meta using the “Manage Future Activity” option, which will also result in the disconnection of historical third-party activity data from their Meta account,²⁸⁶ or alternatively “turn off” storage of future connections between their Meta account and their activities off Meta on a website-by-website or app-by-app basis using the “Disconnect Specific Activity” option (see **Figure 31** and **Figure 32**).

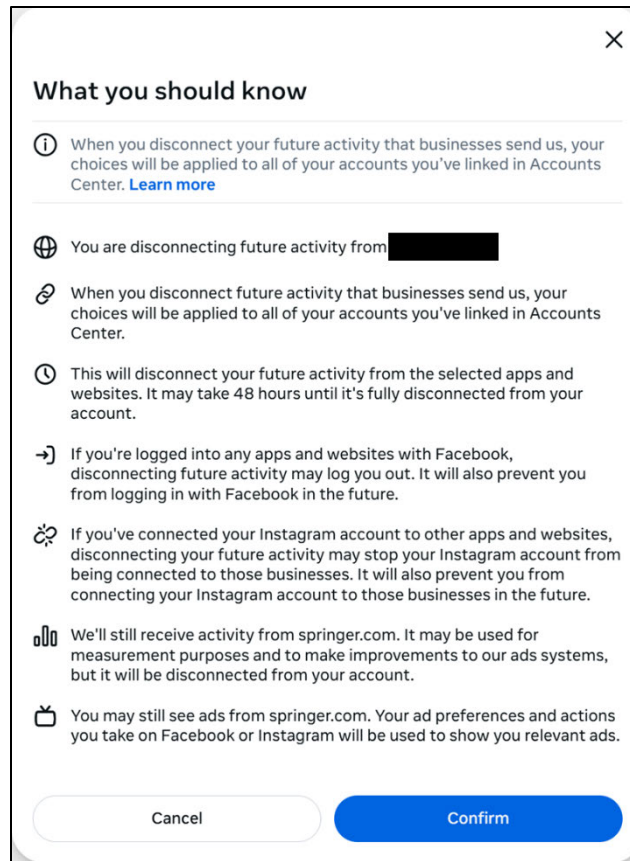
²⁸⁴ See PIXEL_TAX000058869–870 at 870 (“In order for a user to be served Online Behavioral Advertising, we must verify data usage permissions from the user at two points in time: 1. Time of Data Collection: The user must not be opted out through any opt out mechanism at the time of data collection for the OBA data to be used for any personalized ad delivery. 2. Time of Ad Delivery: The user must not be opted out at the time of ad delivery for any OBA data to be used for personalized ad delivery.”)

²⁸⁵ See PIXEL_TAX000052115–123. See also, PIXEL_TAX000052250 at 250 (“You can review your Off-Facebook activity, which is a summary of activity that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites. They use our business tools, such as Meta Pixel, to share this information with us.”).

²⁸⁶ “Manage Your Future Activity Off Meta Technologies,” *Meta Help Center*, <https://www.facebook.com/help/1224342157705160/>, accessed October 25, 2025 (“When [users] turn off [their] future activity off Meta technologies[;] [Users] future activity off Meta technologies will be disconnected within 48 hours from when it’s received. [...] If [users] choose to turn off [their] future activity for all apps and websites, [that will] also disconnect all [their] past activity off Meta technologies.”).

Figure 31: OFA Controls for a User Account²⁸⁷

²⁸⁷ “Your Activity Off Meta Technologies,” *Meta*, https://www.facebook.com/off_facebook_activity/, accessed October 25, 2025.

Figure 32: OFA Controls for a User Account to Disconnect Specific Activity²⁸⁸

120. Meta stores a “separable identifier” or “SID” in association with event data. The SID is used in internal Meta databases to “connect” event data to a Facebook ID.²⁸⁹ When a user “[c]lear[s] previous activity” data from their Facebook/Instagram user accounts,²⁹⁰ Meta “disconnects” the event data from the user’s Facebook/Instagram user ID by resetting the user’s

²⁸⁸ This figure was obtained at my direction by logging in to a Facebook user account and accessing OFA controls for “disconnect[ing] specific activity.”

²⁸⁹ See Patel, Mayur, et al., “Redesigning Our Systems to Provide More Control over Off-Facebook Activity,” *Engineering at Meta*, August 20, 2019, <https://engineering.fb.com/2019/08/20/core-infra/off-facebook-activity/>, accessed September 17, 2025 (“Challenge #2: Disconnecting the data [:] The data warehouse was not designed for deleting or updating individual rows. [...] Since deleting or updating individual rows in real time is not feasible, we had to find a solution [...] We implemented these decisions in part by allocating a new separable identifier (SID) for each person, then replacing UID [(User Identifier)] keys with SIDs. We then created a separate mapping between SIDs and UIDs that can be accessed when data is processed.”).

²⁹⁰ “Your Activity Off Meta Technologies,” *Meta*, https://www.facebook.com/off_facebook_activity/, accessed October 25, 2025.

SID.²⁹¹ When a user “manage[s] future activity,” Meta “disconnects” event data from the user’s Facebook/Instagram ID and prevents future “connections” between incoming event data and the user’s Facebook/Instagram ID by automatically resetting the user’s SID daily.²⁹² Disconnecting OFA allows users to reset the history associated with their SID and break Meta’s ability to maintain continuity of past associations.²⁹³

IX. MR. ZEIDMAN MISCHARACTERIZED THE TECHNICAL NATURE OF THE ALLEGED PEN REGISTER DATA

121. Mr. Zeidman claimed the data produced by Meta includes “pen register” information, such as the webpages members of the proposed classes visited, the date and time of their visits, operating system and browser information, device type, IP address, and geolocation data.²⁹⁴ He further claimed that such “‘pen register’ data is transmitted to Meta each time a person visits a website employing the Meta Pixel.”²⁹⁵ I was asked by counsel to evaluate whether all data Mr. Zeidman characterizes as “pen register” information is necessary for addressing or routing

²⁹¹ See “Redesigning Our Systems to Provide More Control over Off-Facebook Activity,” *Engineering at Meta*, August 20, 2019, <https://engineering.fb.com/2019/08/20/core-infra/off-facebook-activity/>, accessed September 17, 2025 (“If a person chooses to have off-site activity disconnected going forward, we automatically disconnect it and rotate SIDs on a daily basis.”).

²⁹² See “Manage Your Future Activity Off Meta Technologies,” *Meta Help Center*, <https://www.facebook.com/help/1224342157705160/>, accessed October 25, 2025 (“You can also choose to disconnect your activity off Meta technologies, which will disconnect your past activity from your account. Keep in mind, when you turn off future activity for all apps and websites, it’ll also disconnect your past activity.”). See also, “Redesigning Our Systems to Provide More Control over Off-Facebook Activity,” *Engineering at Meta*, August 20, 2019, <https://engineering.fb.com/2019/08/20/core-infra/off-facebook-activity/>, accessed September 17, 2025 (“If a person chooses to have off-site activity disconnected going forward, we automatically disconnect it and rotate SIDs on a daily basis.”).

²⁹³ See “Redesigning Our Systems to Provide More Control over Off-Facebook Activity,” *Engineering at Meta*, August 20, 2019, <https://engineering.fb.com/2019/08/20/core-infra/off-facebook-activity/>, accessed September 17, 2025 (“We then created a separate mapping between SIDs and UIDs that can be accessed when data is processed. In most cases, when a person uses Off-Facebook Activity to disconnect that information, we remove this mapping between the UID and SID within 48 hours, which breaks the process of joining individual rows in data warehouse tables with a user account. [...] We then generate a new SID to be associated with the person’s account going forward.”).

²⁹⁴ Zeidman Report, ¶ 28.

²⁹⁵ Zeidman Report, ¶ 29.

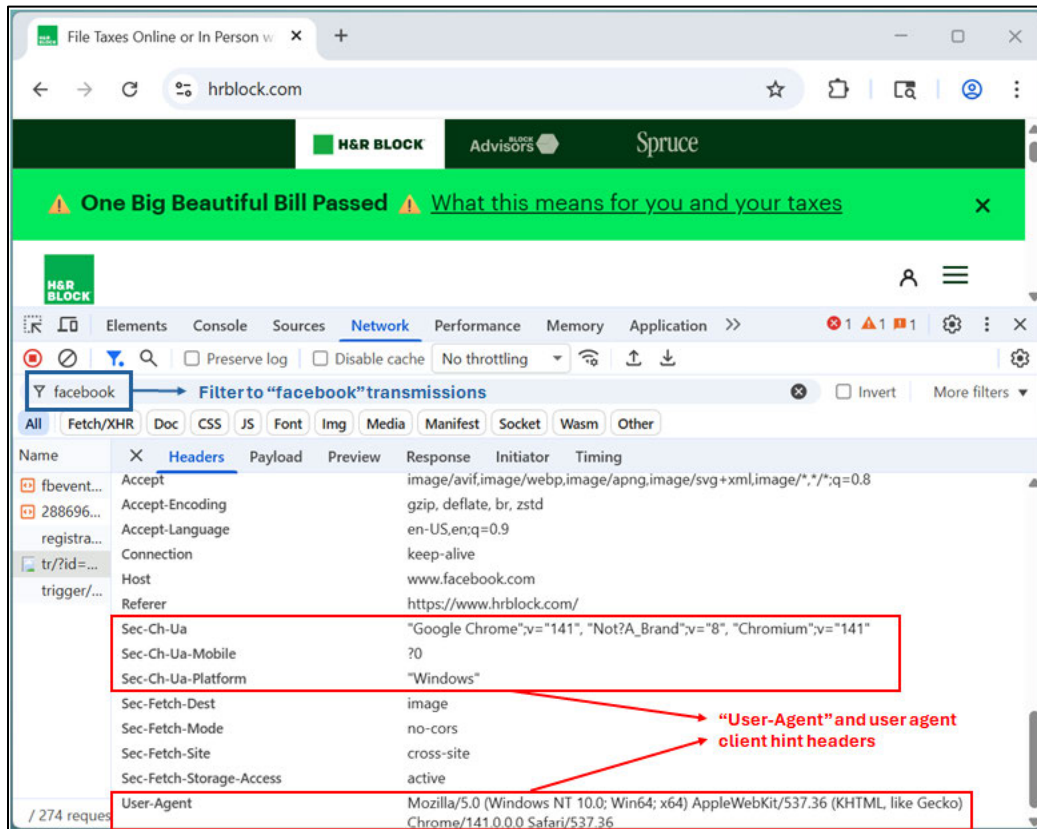
communications. I conclude that certain metadata and inferred data Mr. Zeidman claims are “pen register” data, as a technical matter, are not required for web transmissions to occur.

122. Mr. Zeidman claimed that data typical to HTTP headers, such as browser, device, and operating system information, is “pen register” data.²⁹⁶ These values often appear in the “User-Agent” header and in user agent client hint headers,²⁹⁷ which are strings contained in HTTP requests that can be used to identify the browser and associated operating system sending the requests. While such information can help websites optimize or customize content, these headers are not required and play no role in whether a communication is transmitted from one point to another.²⁹⁸ To demonstrate this, I conducted a test, detailed in Technical **Appendix D**, in which I visited *hrblock.com* while removing the information from these headers. The page loaded successfully and Meta Pixel transmissions still occurred, confirming that these headers were not needed to establish or complete a communication (see **Figure 33** and **Figure 34**). From a technical perspective, data typical to HTTP headers, such as browser, device, and operating system information, are metadata and are not required for web transmissions to occur.

²⁹⁶ Zeidman Report, ¶¶ 27–29.

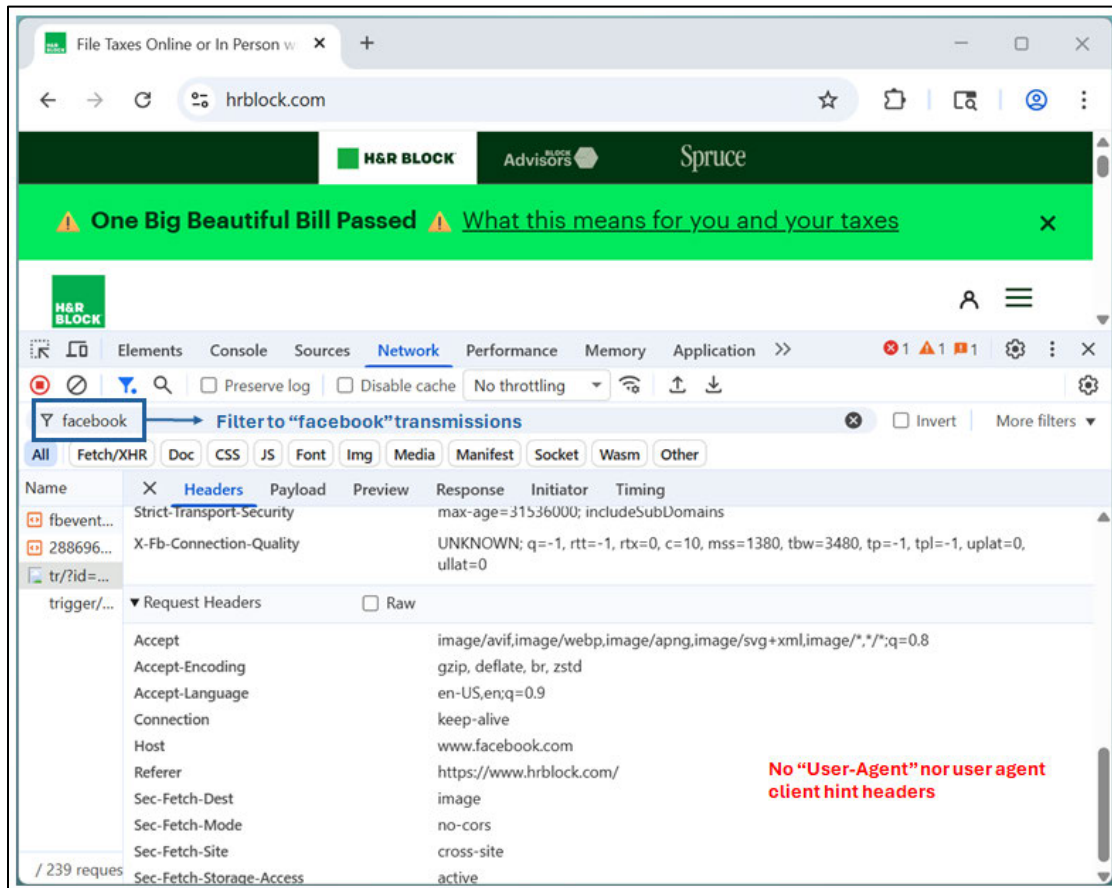
²⁹⁷ User agent client hint headers, like [REDACTED] allow browsers to provide browser, device, and operating system information. They include, among others, “Sec-Ch-Ua,” “Sec-Ch-Ua-Mobile,” and “Sec-Ch-Ua-Platform.” See **Appendix D**. See also, “HTTP Client Hints,” *Mozilla Developer Network*, https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Client_hints, accessed October 20, 2025.

²⁹⁸ HTTP transmissions rely on a TCP (“Transmission Control Protocol”) to establish a connection between the user’s device and a server. This connection does not rely on the “User-Agent” header. See “TCP (Transmission Control Protocol) – The Transmission Protocol Explained,” *Ionos*, March 2, 2020, <https://www.ionos.com/digitalguide/server/know-how/introduction-to-tcp/>, accessed October 20, 2025 (“Prerequisites for establishing a valid TCP connection: Both endpoints must already have a unique IP address (IPv4 or IPv6) and have assigned and enabled the desired port for data transfer. The IP address serves as an identifier, whereas the port allows the operating system to assign connections to the specific client and server applications.”).

Figure 33: Visiting *hrblock.com* Without Modifying the “User-Agent” or User Agent Client Hint Headers²⁹⁹

²⁹⁹ See Appendix D; “windows_chrome_hrblock_default.har” in my produced backup materials.

Figure 34: Visiting *hrblock.com* After Modifying the “User-Agent” and User Agent Client Hint Headers³⁰⁰



123. Moreover, when Mr. Zeidman characterized the alleged “pen-register” data, he claimed that “geolocation data” was “transmitted” to Meta “like other ‘pen register’ data.”³⁰¹ In doing so, Mr. Zeidman mischaracterized the “geolocation data” as data transmitted from the client side to Meta. However, the schema for the [REDACTED] data indicates that [REDACTED] and [REDACTED] fields are [REDACTED] and that the [REDACTED] field is [REDACTED].³⁰² Moreover, Mr. Zeidman contradicted himself by stating that [REDACTED]

³⁰⁰ See Appendix D; [REDACTED].

³⁰¹ Zeidman Report, ¶ 29 [REDACTED],” see Exhibit F at 6, 21 (Ex. 148 to 30(b)(6) deposition), [REDACTED]).

³⁰² PIXEL_TAX000058844.

Highly Confidential – Attorneys’ Eyes Only

█ such as █ and █ was transmitted to Meta³⁰³, only to also admit that these fields were not transmitted but inferred from IP addresses.³⁰⁴

Signed on the 27th day of October, 2025.



Georgios Zervas

³⁰³ Zeidman Report, ¶ 29 █ see Exhibit F at 6, 21 (Ex. 148 to 30(b)(6) deposition), █”).

³⁰⁴ Zeidman Report, ¶ 29 █ ’ Exhibit H (PIXEL TAX000058898–905) at 1–2.”) and Exhibit H █ Zeidman Deposition, at 155:1–8 █